



Cisco ONS 15530 Troubleshooting Guide

Cisco IOS Release 12.2 SV
February 2006

Corporate Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Text Part Number: OL-9544-01



THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Cisco's installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

Modifying the equipment without Cisco's written authorization may result in the equipment no longer complying with FCC requirements for Class A or Class B digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the Cisco equipment or one of its peripheral devices. If the equipment causes interference to radio or television reception, try to correct the interference by using one or more of the following measures:

- Turn the television or radio antenna until the interference stops.
- Move the equipment to one side or the other of the television or radio.
- Move the equipment farther away from the television or radio.
- Plug the equipment into an outlet that is on a different circuit from the television or radio. (That is, make certain the equipment and the television or radio are on circuits controlled by different circuit breakers or fuses.)

Modifications to this product not authorized by Cisco Systems, Inc. could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0601R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Cisco ONS 15530 Troubleshooting Guide

© 2006 Cisco Systems, Inc. All rights reserved.



Preface xix

Document Objectives	xix
Audience	xix
New and Changed Information	xx
Document Organization	xx
Related Documentation	xxi
Document Conventions	xxii
Where to Find Safety and Warning Information	xxiii
Obtaining Documentation	xxiii
Cisco.com	xxiv
Product Documentation DVD	xxiv
Cisco Optical Networking Product Documentation CD-ROM	xxiv
Ordering Documentation	xxiv
Documentation Feedback	xxiv
Cisco Product Security Overview	xxv
Reporting Security Problems in Cisco Products	xxv
Obtaining Technical Assistance	xxvi
Cisco Technical Support & Documentation Website	xxvi
Submitting a Service Request	xxvii
Definitions of Service Request Severity	xxvii
Obtaining Additional Publications and Information	xxvii

CHAPTER 1

Troubleshooting Overview 1-1

1.1 Overview	1-1
1.2 General Model of Problem Solving	1-2
1.3 Maintaining Network Information	1-4
1.4 Network and System Management	1-4
1.4.1 CiscoView	1-4
1.4.2 CTM	1-4
1.4.3 DFM	1-5
1.5 Third-Party Troubleshooting Tools	1-5
1.6 Using General Diagnostic Commands	1-6
1.6.1 show Commands	1-6

- 1.6.2 debug Commands **1-7**
- 1.6.3 ping Command **1-7**
- 1.6.4 traceroute Command **1-8**
- 1.7 Online Diagnostics **1-8**
 - 1.7.1 Accessibility Test **1-8**
 - 1.7.2 OIR Test **1-9**
- 1.8 Configuring Online Diagnostics **1-9**
 - 1.8.1 Displaying the Online Diagnostics Configuration and Results **1-10**
- 1.9 Power-On Diagnostics **1-11**
 - 1.9.1 Configuring Power-On Diagnostics **1-11**
 - 1.9.2 Displaying the Power-On Diagnostic Test Results **1-12**
- 1.10 Checking Release Notes for Workarounds **1-16**
 - 1.10.1 Using Bug Toolkit **1-17**
 - 1.10.2 Checking Cisco IOS Release Notes **1-17**
- 1.11 Initial Troubleshooting Checklist **1-18**

CHAPTER 2

Troubleshooting CPU Switch Module Problems 2-1

- 2.1 Overview **2-1**
- 2.2 Initial Troubleshooting Checklist **2-2**
- 2.3 Verifying CPU Switch Module Configuration **2-2**
- 2.4 Recovering a Lost Password **2-4**
- 2.5 Verifying NME Interface Configurations **2-5**
- 2.6 Troubleshooting CPU Switch Module Memory **2-9**
- 2.7 Verifying Hardware and Software Versions **2-9**
- 2.8 Verifying Hardware and Software Compatibility **2-13**
- 2.9 Troubleshooting Redundant CPU Switch Modules **2-15**
 - 2.9.1 Verifying Hardware and Software Versions of Redundant CPU Switch Modules **2-16**
 - 2.9.2 Verifying Redundant CPU Switch Module Functions **2-19**
- 2.10 Troubleshooting CPU Switch Module Problems **2-22**
 - 2.10.1 Active CPU Switch Module Boot Failure **2-22**
 - 2.10.2 Standby CPU Switch Module Boot Failure **2-23**
 - 2.10.3 Unable to Access CPU Switch Module Console **2-23**
 - 2.10.4 Unable to Access Enable Mode on Active CPU Switch Module **2-23**
 - 2.10.5 Unable to Access Enable Mode on Standby CPU Switch Module **2-24**

CHAPTER 3

Troubleshooting Transponder Line Card Problems 3-1

- 3.1 Overview **3-1**

- 3.2 Initial Troubleshooting Checklist **3-2**
- 3.3 Troubleshooting Transponder Line Card Problems **3-3**
 - 3.3.1 Transponder Line Card Not in show hardware Command Output **3-3**
 - 3.3.2 Wave Interface Is Down and Shows Loss of Light **3-3**
 - 3.3.3 Transparent Interface Is Down and Shows Loss of Light **3-4**
 - 3.3.4 Active and Standby Wavepatch Interfaces Down Due to Loss of Light **3-4**
 - 3.3.5 Wave Interface Shows Loss of Lock **3-5**
 - 3.3.6 Transparent Interface Shows Loss of Lock **3-5**
 - 3.3.7 Interface Shows Loss of Sync **3-5**
 - 3.3.8 Interface Shows Loss of Frame **3-6**
 - 3.3.9 Active and Standby Wavepatch Interfaces Down Due to Low Alarm **3-6**
 - 3.3.10 Unable to Configure Protocol Encapsulation or Clock Rate **3-6**
- 3.4 Troubleshooting Transponder Line Card Problems Using Loopbacks **3-7**
 - 3.4.1 Client Signal Loopbacks **3-7**
 - Procedure: Create a Client Signal Loopback **3-8**
 - 3.4.2 Trunk Loopbacks **3-8**
 - Procedure: Create a Trunk Loopback **3-9**

CHAPTER 4**Troubleshooting ESCON Aggregation Card Problems 4-1**

- 4.1 Overview **4-1**
- 4.2 Initial Troubleshooting Checklist **4-2**
- 4.3 Troubleshooting ESCON Aggregation Card Interface Problems **4-3**
 - 4.3.1 Removing an SFP Optics Causes Alarms on Other Esconphy Interfaces **4-3**
 - 4.3.2 **Shutting Down** One Esconphy Interface Raises Alarms on Other Esconphy Interfaces **4-3**
 - 4.3.3 Reenabling an Esconphy Interface Clears Alarms on Other Esconphy Interfaces **4-4**
 - 4.3.4 All Client Side Lasers Shut Down When Traffic to One Esconphy Interface Falls Below a Threshold **4-4**
 - 4.3.5 Client Side Laser Unexpectedly Shuts Down **4-4**
 - 4.3.6 Client Traffic Does Not Flow End-to-End **4-5**
 - 4.3.7 Portgroup Interface Shows Continuous Errors **4-6**
 - 4.3.8 Esconphy Interface Not Created **4-6**
- 4.4 Troubleshooting ESCON Aggregation Card Problems Using Loopbacks **4-7**
 - 4.4.1 Client Signal Loopbacks **4-7**
 - Procedure: Create a Client Signal Loopback **4-7**

CHAPTER 5**Troubleshooting 4-Port 1-Gbps/2-Gbps FC Aggregation Card Problems 5-1**

- 5.1 Overview **5-1**
- 5.2 Initial Troubleshooting Checklist **5-2**
- 5.3 Troubleshooting 4-Port 1-Gbps/2-Gbps FC Aggregation Card Interface Problems **5-3**

- 5.3.1 FC/FICON Encapsulated Twogigabitphy Interface Is Down **5-3**
- 5.3.2 Twogigabitphy Interface Is Administratively Down **5-3**
- 5.3.3 Client Equipment Interface Connected to the 4-Port 1-Gbps/2-Gbps FC Aggregation Card Is Not Up **5-4**
- 5.3.4 Client Equipment Detects CVRD Errors **5-5**
- 5.3.5 Transmit Frame Count Is Not Incrementing **5-5**
- 5.3.6 FC/FICON Encapsulated Twogigabitphy Interface Receives CRC Errors from Trunk Card **5-6**
- 5.3.7 Both the Local and Remote Twogigabitphy Interfaces Are Down **5-7**
- 5.3.8 Twogigabitphy Interface Not Created **5-7**
- 5.3.9 Twogigabitphy Interface Reports Loss of Sync **5-8**
- 5.3.10 Throughput Is Low **5-8**
- 5.3.11 Throughput Is Asymmetric **5-9**
- 5.3.12 Flow Control Is Inactive **5-10**
- 5.3.13 Oversubscribed Portgroup and Superportgroup Related Problems Are Experienced **5-10**
- 5.4 Troubleshooting Problems Using show controller Command Output **5-11**
- 5.5 Troubleshooting 4-Port 1-Gbps/2-Gbps FC Aggregation Card Problems Using Loopbacks **5-16**
 - 5.5.1 Facility Loopbacks **5-16**
 - Procedure: Create a Facility Loopback **5-17**
 - 5.5.2 Terminal Loopbacks **5-17**
 - Procedure: Create a Terminal Loopback **5-18**

CHAPTER 6

Troubleshooting 8-Port FC/GE Aggregation Card Problems 6-1

- 6.1 Overview **6-1**
- 6.2 Initial Troubleshooting Checklist **6-2**
- 6.3 Troubleshooting 8-Port FC/GE Aggregation Card Interface Problems **6-3**
 - 6.3.1 FC/FICON Encapsulated Gigabitphy Interface Is Down **6-3**
 - 6.3.2 GE Encapsulated Gigabitphy Interface Is Down **6-3**
 - 6.3.3 Gigabitphy Interface Is Administratively Down **6-4**
 - 6.3.4 Client Equipment Interface Connected to the 8-Port FC/GE Aggregation Card Is Not Up **6-5**
 - 6.3.5 Client Equipment Detects CVRD Errors **6-5**
 - 6.3.6 Transmit Frame Count Is Not Incrementing **6-6**
 - 6.3.7 Local Interface with GE Encapsulation Receives Frames But Not the Remote Interface **6-7**
 - 6.3.8 FC/FICON Encapsulated Gigabitphy Interface Receives CRC Errors from Trunk Card **6-7**
 - 6.3.9 Both the Local and Remote Gigabit Interfaces Are Down **6-8**
 - 6.3.10 Gigabitphy Interface Not Created **6-8**
- 6.4 Debugging Problems Using show controller Command Output **6-9**
- 6.5 Troubleshooting 8-Port FC/GE Aggregation Card Problems Using Loopbacks **6-11**
 - 6.5.1 Facility Loopbacks **6-11**
 - 6.5.2 Terminal Loopbacks **6-12**

CHAPTER 7**Troubleshooting 8-Port Multi-Service Muxponder Problems 7-1**

- 7.1 Overview **7-1**
- 7.2 Initial Troubleshooting Checklist **7-2**
- 7.3 Troubleshooting Multirate Interface Problems **7-2**
 - 7.3.1 Loss of Light on Multirate Interfaces **7-3**
 - 7.3.2 Loss of Sync on Multirate Interfaces **7-3**
 - 7.3.3 Loss of Lock on Multirate Interfaces **7-4**
 - 7.3.4 Loss of Signal on Multirate Interfaces **7-4**
 - 7.3.5 AIS Error on Multirate Interface Encapsulated for T1 or E1 **7-4**
 - 7.3.6 Multirate Interface Displays Remote Client Error Message **7-5**
 - 7.3.7 Multirate Interface Detects CVRD Errors **7-5**
 - 7.3.8 Multirate Interface Not Appearing In Configuration **7-6**
 - 7.3.9 Encapsulation is Rejected on the Multirate Interface **7-6**
- 7.4 Troubleshooting Trunk-Side Interfaces **7-7**
 - 7.4.1 Wavesonetphy Interface Down and Shows Loss of Lock **7-7**
 - 7.4.2 Wavesonetphy Interface Down and Shows Loss of Frame **7-7**
 - 7.4.3 B1 Errors on the Wavesonetphy Interface **7-8**
 - 7.4.4 Sdcc Interface Down **7-8**
- 7.5 Troubleshooting TSI Protocol Problems **7-9**
 - 7.5.1 End-to-End Traffic Not Flowing Due to TSI Problems **7-9**
- 7.6 Troubleshooting 8-Port Multi-Service Muxponder Problems Using Loopbacks **7-10**
 - 7.6.1 Client-Side Facility Loopbacks **7-10**
 - 7.6.2 Client-Side Terminal Loopbacks **7-11**
 - 7.6.3 Trunk-Side Facility Loopbacks **7-11**
 - 7.6.4 Trunk-Side Terminal Loopbacks **7-12**
 - 7.6.5 Troubleshooting Protocol Level Errors in an End-to-End Scenario **7-13**

CHAPTER 8**Troubleshooting 2.5-Gbps ITU Trunk Card Problems 8-1**

- 8.1 Overview **8-1**
- 8.2 Initial Troubleshooting Checklist **8-2**
- 8.3 Troubleshooting 2.5-Gbps ITU Trunk Card Interface Problems **8-3**
 - 8.3.1 Waveethernetphy Interface Down and Shows Loss of Lock **8-3**
 - 8.3.2 Waveethernetphy Interface Down and Shows Loss of Sync **8-3**
 - 8.3.3 CVRD Errors on the Waveethernetphy Interface **8-4**
 - 8.3.4 CRC and CDL HEC Errors on the Waveethernetphy Interface **8-4**
 - 8.3.5 Ethernetdcc Interface Down **8-5**
- 8.4 Troubleshooting 2.5-Gbps ITU Trunk Card Problems Using Loopbacks **8-5**
 - 8.4.1 Facility Loopbacks **8-5**

Procedure: Create a Facility Loopback 8-6
 8.4.2 Terminal Loopbacks 8-6

CHAPTER 9

Troubleshooting 10-Gbps ITU Trunk Card Problems 9-1

9.1 Overview 9-1
 9.2 Initial Troubleshooting Checklist 9-3
 9.3 Troubleshooting 10-Gbps ITU Trunk Card Interface Problems 9-3
 9.3.1 Waveethernetphy Interface Down and Shows Loss of Lock 9-3
 9.3.2 Waveethernetphy Interface Down and Shows Loss of Sync 9-4
 9.3.3 CVRD Errors on the Waveethernetphy Interface 9-4
 9.3.4 CRC and CDL HEC Errors on the Waveethernetphy Interface 9-5
 9.3.5 Ethernetdcc Interface Down 9-5
 9.4 Troubleshooting 10-Gbps ITU Trunk Card Problems Using Loopbacks 9-5
 9.4.1 Facility Loopbacks 9-5
 9.4.2 Terminal Loopbacks 9-6

CHAPTER 10

Troubleshooting 10-Gbps ITU Tunable Trunk Card Problems 10-1

10.1 Overview 10-1
 10.2 Initial Troubleshooting Checklist 10-3
 10.3 Troubleshooting 10-Gbps ITU Tunable Trunk Card Interface Problems 10-3
 10.3.1 Waveethernetphy Interface Down and Shows Loss of Lock 10-3
 10.3.2 Waveethernetphy Interface Down and Shows Loss of Sync 10-4
 10.3.3 CVRD Errors on the Waveethernetphy Interface 10-4
 10.3.4 CRC and CDL HEC Errors on the Waveethernetphy Interface 10-5
 10.3.5 Ethernetdcc Interface Down 10-5
 10.4 Troubleshooting 10-Gbps ITU Tunable Trunk Card Problems Using Loopbacks 10-6
 10.4.1 Facility Loopbacks 10-6
 10.4.2 Terminal Loopbacks 10-7

CHAPTER 11

Troubleshooting 10-Gbps Uplink Card Problems 11-1

11.1 Overview 11-1
 11.2 Initial Troubleshooting Checklist 11-2
 11.3 Troubleshooting 10-Gbps Uplink Card Interface Problems 11-2
 11.3.1 Tengigethernetphy Interface Down and Shows Loss of Lock 11-3
 11.3.2 Tengigethernetphy Interface Down and Shows Loss of Sync 11-3
 11.3.3 Ethernetdcc Interface Down 11-3
 11.4 Troubleshooting 10-Gbps Uplink Card Problems Using Loopbacks 11-4
 11.4.1 Facility Loopbacks 11-4

11.4.2 Terminal Loopbacks 11-5

CHAPTER 12**Troubleshooting OADM Module Problems 12-1**

12.1 Overview 12-1

12.2 Initial Troubleshooting Checklist 12-2

12.3 Troubleshooting OADM Module Problems 12-3

12.3.1 OADM Module Is Not Recognized 12-3

12.3.2 OADM Channel Interfaces Are Not Recognized After a CPU Switch Module Switchover 12-3

12.3.3 Waveethernetphy or Wave Interface Is Down 12-3

CHAPTER 13**Troubleshooting PSM Problems 13-1**

13.1 Overview 13-1

13.2 Initial Troubleshooting Checklist 13-1

13.3 Troubleshooting PSM Interface Problems 13-1

13.3.1 Wdmsplit Interface Down 13-2

13.3.2 Wdmsplit Interface Power Level Indicates Loss of Light 13-2

13.3.3 Wdmsplit Interface Receives Light But End Wave Interface Shows Loss of Light 13-2

13.3.4 Wdm Interface Loses Topology Neighbor Learning Via CDP 13-3

13.3.5 Automatic CDP Learning Is Not Enabled on Wdmsplit Interface 13-3

CHAPTER 14**Troubleshooting VOA Module Problems 14-1**

14.1 Overview 14-1

14.2 Initial Troubleshooting Checklist 14-3

14.3 Troubleshooting VOA Module Problems 14-3

14.3.1 Voain Interface Shows Low Optical Alarm Threshold Error 14-4

14.3.2 Voafilterin Subinterface Shows Low Optical Alarm Threshold Error 14-4

14.3.3 Voain Interface Shows High Optical Alarm Threshold Error 14-5

14.3.4 Voafilterin Subinterface Shows High Optical Alarm Threshold Error 14-5

14.3.5 STA LED Continues Blinking After Initialization Complete 14-6

14.3.6 Optical Threshold Warnings Not Reported 14-6

CHAPTER 15**Troubleshooting APS Problems 15-1**

15.1 Overview 15-1

15.2 Initial Troubleshooting Checklist 15-1

15.3 Troubleshooting Specific APS Problems 15-2

15.3.1 APS Group State Enabled But Not Associated 15-2

15.3.2 Bidirectional APS Configured But Remote Node Direction, Architecture, and Receive k1/k2 Are Unknown 15-2

- 15.3.3 Message Channel Interface Up But APS Msg-Channel Status Down **15-3**
- 15.3.4 APS Does Not Switch to Protection Signal When the Working Signal Fails **15-4**
- 15.3.5 Lockout from Protection Request Fails **15-4**
- 15.3.6 Several Unexpected APS Messages Received **15-5**
- 15.3.7 Remote Switchover Does Not Occur After Local Switchover **15-5**
- 15.3.8 Manual or Forced Switchover Fails **15-6**
- 15.3.9 Wave Interface or Waveethernetphy Interface Is Down and One Wavepatch Interface Is Up **15-6**
- 15.3.10 APS Group Transmitting k1k2 sf-lp to Peer APS Group **15-6**

CHAPTER 16

Troubleshooting OSCP Problems 16-1

- 16.1 Overview **16-1**
- 16.2 Initial Troubleshooting Checklist **16-1**
- 16.3 Troubleshooting OSCP Problems **16-1**
 - 16.3.1 OSC Wave Interface Down **16-2**
 - 16.3.2 EthernetDcc Interface Down **16-2**
 - 16.3.3 EthernetDcc Interface Is Up But Line Protocol Is Down **16-2**

CHAPTER 17

Troubleshooting Threshold Alarms 17-1

- 17.1 Initial Troubleshooting Checklist **17-1**
- 17.2 Troubleshooting Threshold Alarms **17-1**
 - 17.2.1 8b10b CVRD Alarm Indicates Signal Fail or Signal Degrade **17-1**
 - 17.2.2 CDL HEC Alarm Indicates Signal Fail or Signal Degrade **17-2**
 - 17.2.3 64b66b CVRD Alarm Indicates Signal Fail or Signal Degrade **17-3**
 - 17.2.4 B1 CVRD Alarm Indicates Signal Fail or Signal Degrade **17-3**
 - 17.2.5 Threshold Exceeded Messages Continuously Hitting the Console **17-4**
 - 17.2.6 SNMP Traps Are Not Generated **17-4**

CHAPTER 18

Troubleshooting Performance History Counter Problems 18-1

- 18.1 Overview **18-1**
- 18.2 Initial Troubleshooting Checklist **18-1**
- 18.3 Interpreting Performance History Messages **18-2**
- 18.4 Troubleshooting Performance History Counters **18-2**
 - 18.4.1 Some Counters Are Not Displayed **18-2**
 - 18.4.2 Performance History Counters Are Not Preserved Across CPU Switch Module Switchovers **18-3**

APPENDIX A**Technical Support A-1**

- A.1 Gathering Information About Your Internetwork **A-1**
 - A.1.1 Getting the Data from Your System **A-2**
- A.2 Providing Data to Customer Service **A-2**

INDEX



FIGURES

<i>Figure 1-1</i>	Cisco ONS 15530	1-2
<i>Figure 1-2</i>	General Model of Problem Solving	1-3
<i>Figure 3-1</i>	Transponder Line Card Architecture	3-2
<i>Figure 3-2</i>	Transponder Line Card Interfaces	3-2
<i>Figure 3-3</i>	Client Signal Loopback Example	3-7
<i>Figure 3-4</i>	Trunk Loopback Example	3-8
<i>Figure 4-1</i>	Interface Model for ESCON Aggregation	4-2
<i>Figure 4-2</i>	Client Signal Loopback Example	4-7
<i>Figure 5-1</i>	Interfaces for a 4-port 1-Gbps/2-Gbps FC Aggregation Card	5-2
<i>Figure 5-2</i>	Facility Loopback Example	5-17
<i>Figure 5-3</i>	Terminal Loopback Example	5-18
<i>Figure 6-1</i>	Interfaces for an 8-Port FC/GE Aggregation Card	6-2
<i>Figure 6-2</i>	Facility Loopback Example	6-11
<i>Figure 6-3</i>	Terminal Loopback Example	6-12
<i>Figure 7-1</i>	8-Port Multi-Service Muxponder Interfaces (Splitter Shown)	7-2
<i>Figure 7-2</i>	Client-Side Facility Loopback Example	7-10
<i>Figure 7-3</i>	Client-Side Terminal Loopback Example	7-11
<i>Figure 7-4</i>	Trunk-Side Facility Loopback Example	7-12
<i>Figure 7-5</i>	Trunk-Side Terminal Loopback Example	7-13
<i>Figure 7-6</i>	8-Port Multi-Service Muxponders in an End-to-End Configuration	7-13
<i>Figure 8-1</i>	Splitter 2.5-Gbps ITU Trunk Card Interfaces	8-2
<i>Figure 8-2</i>	Nonsplitter 2.5-Gbps ITU Trunk Card Interfaces	8-2
<i>Figure 8-3</i>	Facility Loopback Example on a 2.5-Gbps ITU Trunk Card	8-6
<i>Figure 8-4</i>	Terminal Loopback Example on a 2.5-Gbps ITU Trunk Card	8-7
<i>Figure 9-1</i>	Splitter 10-Gbps ITU Trunk Card Interfaces	9-2
<i>Figure 9-2</i>	Nonsplitter 10-Gbps ITU Trunk Card Interfaces	9-2
<i>Figure 9-3</i>	Facility Loopback Example on a 10-Gbps ITU Trunk Card	9-6
<i>Figure 9-4</i>	Terminal Loopback Example on a 10-Gbps ITU Trunk Card	9-7
<i>Figure 10-1</i>	Splitter 10-Gbps ITU Tunable Trunk Card Interfaces	10-2
<i>Figure 10-2</i>	Nonsplitter 10-Gbps ITU Tunable Trunk Card Interfaces	10-2
<i>Figure 10-3</i>	Facility Loopback Example on a 10-Gbps ITU Tunable Trunk Card	10-6

<i>Figure 10-4</i>	Terminal Loopback Example on a 10-Gbps ITU Tunable Trunk Card	10-7
<i>Figure 11-1</i>	10-Gbps Uplink Card Interfaces	11-2
<i>Figure 11-2</i>	Facility Loopback Example on a 10-Gbps Uplink Card	11-4
<i>Figure 11-3</i>	Terminal Loopback Example on a 10-Gbps Uplink Card	11-5
<i>Figure 12-1</i>	OADM Module Architecture	12-2
<i>Figure 14-1</i>	Single WB-VOA Module Interfaces	14-1
<i>Figure 14-2</i>	Dual WB-VOA Module Interfaces	14-2
<i>Figure 14-3</i>	Single PB-OE Module Interfaces	14-2
<i>Figure 14-4</i>	Dual PB-OE Module Interfaces	14-3



TABLES

Table 1-1	Useful Diagnostic Commands	1-6
Table 2-1	Active CPU Switch Module Boot Failure	2-22
Table 2-2	Standby CPU Switch Module Boot Failure	2-23
Table 2-3	Unable to Access Switch Module Console	2-23
Table 2-4	Unable to Access Enable Mode	2-23
Table 2-5	Unable to Access Enable Mode	2-24
Table 3-1	Transponder Line Card Not in show hardware Command Output	3-3
Table 3-2	Wave Interface Is Down and Shows Loss of Light	3-4
Table 3-3	Transparent Interface Down and Shows Loss of Light	3-4
Table 3-4	Wavepatch Interfaces Down Due to Loss of Light	3-4
Table 3-5	Wave Interface Shows Loss of Lock	3-5
Table 3-6	Wave Interface Shows Loss of Lock	3-5
Table 3-7	Interface Shows Loss of Sync	3-5
Table 3-8	Interface Shows Loss of Frame	3-6
Table 3-9	Active and Standby Wavepatch Interfaces Down Due to Low Alarm	3-6
Table 3-10	Unable to Configure Protocol Encapsulation or Clock Rate	3-7
Table 3-11	Client Signal Loopback Fails	3-8
Table 3-12	Trunk Loopback Fails	3-9
Table 4-1	Removing an SFP Optics Causes Alarms on Other Esconphy Interfaces	4-3
Table 4-2	Shutting Down One Esconphy Interface Raises Alarms on Other Esconphy Interfaces	4-3
Table 4-3	Reenabling an Esconphy Interface Clears Alarms on Other Esconphy Interfaces	4-4
Table 4-4	All Client Side Lasers Shut Down When Traffic to One Esconphy Interface Falls Below a Threshold	4-4
Table 4-5	Client Side Laser Unexpectedly Shuts Down	4-5
Table 4-6	Client Traffic Does Not Flow End-to-End	4-5
Table 4-7	Portgroup Interface Shows Continuous Errors	4-6
Table 4-8	Esconphy interface not created	4-6
Table 5-1	FC/FICON Encapsulated Twogigabitphy Interface Is Down	5-3
Table 5-2	Twogigabitphy Interface Is Administratively Down	5-4
Table 5-3	Client Equipment Connected to a Twogigabitphy Interface Is Not Up	5-4
Table 5-4	Client Equipment Detects CVRD Errors	5-5
Table 5-5	Transmit Frame Count Is Not Incrementing	5-6

Table 5-6	FC/FICON Encapsulated Twogigabitphy Interface Receives CRC Errors from Trunk Card	5-7
Table 5-7	Both the Local and Remote Gigabit Interfaces Are Down	5-7
Table 5-8	Twogigabitphy Interface Not Created	5-8
Table 5-9	Twogigabitphy Interface Reports Loss of Sync	5-8
Table 5-10	Throughput Is Low	5-9
Table 5-11	Throughput Is Asymmetric	5-9
Table 5-12	Flow Control Is Inactive	5-10
Table 5-13	Oversubscribed Portgroup and Superportgroup Related Problem Are Experienced	5-10
Table 5-14	show controllers twogigabitphy Command Output Field Descriptions	5-13
Table 5-15	show controllers superportgroup Command Output Field Descriptions	5-14
Table 5-16	show controllers portgroup Command Output Field Descriptions	5-15
Table 6-1	FC/FICON Encapsulated Gigabitphy Interface Is Down	6-3
Table 6-2	GE Encapsulated Gigabitphy Interface Is Down	6-4
Table 6-3	Gigabitphy Interface Is Administratively Down	6-5
Table 6-4	Client Equipment Interface Connected to the 8-Port FC/GE Aggregation Card Is Not Up	6-5
Table 6-5	Client Equipment Detects CVRD Errors	6-6
Table 6-6	Transmit Frame Count Is Not Incrementing	6-6
Table 6-7	Local Interface With GE Encapsulation Receives Frames But Not the Remote Interface	6-7
Table 6-8	FC/FICON Encapsulated Gigabitphy Interface Receives CRC Errors from Line Card	6-8
Table 6-9	Both the Local and Remote Gigabit Interfaces Are Down	6-8
Table 6-10	Gigabitphy interface not created	6-8
Table 6-11	show controllers Command Output Field Descriptions	6-10
Table 7-1	Multirate Interface Is Down Due to Loss of Light	7-3
Table 7-2	Multirate Interface Is Down Due to Loss of Sync	7-3
Table 7-3	Multirate Interface Is Down Due to Loss of Lock	7-4
Table 7-4	Multirate Interface Down Due to Loss of Signal	7-4
Table 7-5	AIS Errors on a Multirate Interface	7-5
Table 7-6	Multirate Interface Displays "Remote Client Error" Message	7-5
Table 7-7	Multirate Interface Detects CVRD Errors	7-6
Table 7-8	Multirate Interface Does Not Appear In Configuration	7-6
Table 7-9	Encapsulation is Rejected on the Multirate Interface	7-6
Table 7-10	Wavesonetphy Interface Down and Shows Loss of Lock	7-7
Table 7-11	Wavesonetphy Interface Down and Shows Loss of Frame	7-8
Table 7-12	Wavesonetphy Interface Shows B1 Errors	7-8
Table 7-13	Sdcc Interface Down	7-8

Table 7-14	End-to-End Traffic Not Flowing Due to TSI Problems	7-9
Table 8-1	Waveethernetphy Interface Down and Shows Loss of Lock	8-3
Table 8-2	Waveethernetphy Interface Down and Shows Loss of Sync	8-4
Table 8-3	CVRD Errors on the Waveethernetphy Interface	8-4
Table 8-4	CRC and CDL HEC Errors on the Waveethernetphy Interface	8-5
Table 8-5	Ethernetdcc Interface Down	8-5
Table 9-1	Waveethernetphy Interface Down and Shows Loss of Lock	9-3
Table 9-2	Waveethernetphy Interface Down and Shows Loss of Sync	9-4
Table 9-3	CVRD Errors on the Waveethernetphy Interface	9-4
Table 9-4	CRC and CDL HEC Errors on the Waveethernetphy Interface	9-5
Table 9-5	Ethernetdcc Interface Down	9-5
Table 10-1	Waveethernetphy Interface Down and Shows Loss of Lock	10-3
Table 10-2	Waveethernetphy Interface Down and Shows Loss of Sync	10-4
Table 10-3	CVRD Errors on the Waveethernetphy Interface	10-5
Table 10-4	CRC and CDL HEC Errors on the Waveethernetphy Interface	10-5
Table 10-5	Ethernetdcc Interface Down	10-5
Table 11-1	Tengigethernetphy Interface Down and Shows Loss of Lock	11-3
Table 11-2	Tengigethernetphy Interface Down and Shows Loss of Sync	11-3
Table 11-3	Ethernetdcc Interface Down	11-3
Table 12-1	OADM Module Not Recognized	12-3
Table 12-2	OADM Channel Interfaces Not Recognized After Switchover	12-3
Table 12-3	Waveethernetphy or Wave Interface Is Down	12-4
Table 13-1	Wdmsplit Interface Is Down	13-2
Table 13-2	Wdmsplit Interface Power Level Indicates Loss of Light	13-2
Table 13-3	Wdmsplit Interface Receives Light But End Wave Interface Shows Loss of Light	13-3
Table 13-4	Wdm Interface Loses Topology Neighbor Learning Via CDP	13-3
Table 13-5	Automatic CDP Learning Is Not Enabled on Wdmsplit Interface	13-3
Table 14-1	Voain Interface Shows Low Optical Alarm Threshold Error	14-4
Table 14-2	Voafilterin Subinterface Shows Low Optical Alarm Threshold Error	14-4
Table 14-3	Voain Interface Shows High Optical Alarm Threshold Error	14-5
Table 14-4	Voafilterin Subinterface Shows High Optical Alarm Threshold Error	14-5
Table 14-5	STA LED Continues Blinking After Initialization Complete	14-6
Table 14-6	Optical Threshold Warnings Not Reported	14-6
Table 15-1	APS Group State Enabled But Not Associated	15-2
Table 15-2	Bidirectional APS Configured But Remote Node Direction, Architecture, and Receive k1/k2 Are Unknown	15-3

Table 15-3	Message Channel Interface Up But APS msg-channel Status Down	15-3
Table 15-4	APS Does Not Switch to Protection Signal When the Working Signal Fails	15-4
Table 15-5	Lockout from Protection Request Fails	15-5
Table 15-6	Several Unexpected APS Messages Received	15-5
Table 15-7	Remote Switchover Does Not Occur After Local Switchover	15-5
Table 15-8	Manual or Forced Switchover Fails	15-6
Table 15-9	Wave Interface or Waveethernetphy Interface Is Down and One Wavepatch Interface Is Up	15-6
Table 15-10	APS Group Transmitting k1k2 sf-lp to Peer APS Group	15-7
Table 16-1	OSC Wave Interface Is Down	16-2
Table 16-2	EthernetDcc Interface Is Down	16-2
Table 16-3	EthernetDcc Interface Is Up But Line Protocol Is Down	16-3
Table 17-1	8b10b CVRD Alarm Indicates Signal Fail or Signal Degrade	17-2
Table 17-2	CDL HEC Alarm Indicates Signal Fail or Signal Degrade	17-3
Table 17-3	64b66b CVRD Alarm Indicates Signal Fail or Signal Degrade	17-3
Table 17-4	B1 CVRD Alarm Indicates Signal Fail or Signal Degrade	17-3
Table 17-5	Threshold Exceeded Messages Continuously Hitting the Console	17-4
Table 17-6	SNMP Traps Are Not Generated	17-4
Table 18-1	Some Counters Are Not Displayed	18-3
Table 18-2	Performance History Counters Are Not Preserved Across CPU Switch Module Switchovers	18-3



Preface

This section explains the objectives, intended audience, and organization of this publication and describes the conventions that convey instructions and other information.

This section provides the following information:

- Document Objectives
- Audience
- New and Changed Information
- Document Organization
- Related Documentation
- Document Conventions
- Where to Find Safety and Warning Information
- Obtaining Documentation
- Documentation Feedback
- Cisco Product Security Overview
- Obtaining Technical Assistance
- Obtaining Additional Publications and Information

Document Objectives

This guide explains the troubleshooting procedures for the Cisco ONS 15530 system. Use this guide in conjunction with the appropriate publications listed in the Related Documentation section.

Audience

To use this publication, you should be familiar with Cisco or equivalent optical transmission hardware and cabling, telecommunications hardware and cabling, electronic circuitry and wiring practices, and preferably have experience as a telecommunications technician.

New and Changed Information

The table in this section lists and briefly describes the ongoing new and changed hardware features for the Cisco ONS 15530 by Cisco IOS software release. Additionally, it shows the location of the new feature information in this guide.

Feature	Release	Description	Location
Support for end-to-end speed negotiation, oversubscription, superportgroup, performance history counters, and SSHv2 on the 4-port 1-Gbps/2-Gbps FC aggregation card.	12.2(29)SV	The Cisco ONS 15530 supports end-to-end speed negotiation, oversubscription, superportgroup, performance history counters, and SSHv2 on the 4-port 1-Gbps/2-Gbps FC aggregation card.	Chapter 5, “Troubleshooting 4-Port 1-Gbps/2-Gbps FC Aggregation Card Problems” Chapter 18, “Troubleshooting Performance History Counter Problems”
8-port multi-service muxponder	12.2(25)SV	The Cisco ONS 15530 supports up to eight ports of client traffic into a 2.5-Gbps DWDM trunk circuit.	Chapter 7, “Troubleshooting 8-Port Multi-Service Muxponder Problems”
4-port 1-Gbps/2-Gbps FC aggregation card	12.2(23)SV	The Cisco ONS 15530 supports the aggregation of four ports of individually configured 1-Gbps/2-Gbps FC, FICON, or ISC-3 links compatibility mode traffic.	Chapter 5, “Troubleshooting 4-Port 1-Gbps/2-Gbps FC Aggregation Card Problems”
8-port FC/GE aggregation card	12.1(12c)EV	The Cisco ONS 15530 supports the 8-port Fibre Channel/Gigabit Ethernet aggregation card for FC (Fibre Channel) and GE (Gigabit Ethernet) traffic.	Chapter 6, “Troubleshooting 8-Port FC/GE Aggregation Card Problems”
2.5-Gbps ITU trunk cards	12.1(12c)EV	The Cisco ONS 15530 supports the 2.5-Gbps ITU trunk card that sends and receives the ITU grid wavelength signal to and from an OADM module.	Chapter 8, “Troubleshooting 2.5-Gbps ITU Trunk Card Problems”
Protection switch module	12.1(12c)EV	The Cisco ONS 15530 supports the PSM (protection switch module) that provides trunk fiber protection.	Chapter 13, “Troubleshooting PSM Problems”

Document Organization

This Cisco ONS 15530 Troubleshooting Guide is organized into the following chapters:

- Chapter 1, “Troubleshooting Overview,” provides an overview of troubleshooting features and functions.
- Chapter 2, “Troubleshooting CPU Switch Module Problems,” describes the troubleshooting procedures used on the CPU switch modules.
- Chapter 3, “Troubleshooting Transponder Line Card Problems,” describes the troubleshooting procedures used for transponder line card problems.
- Chapter 4, “Troubleshooting ESCON Aggregation Card Problems,” describes the troubleshooting procedures used for ESCON aggregation card problems.

- Chapter 5, “Troubleshooting 4-Port 1-Gbps/2-Gbps FC Aggregation Card Problems,” describes the troubleshooting procedures used for 4-port 1-Gbps/2-Gbps FC aggregation card problems.
- Chapter 6, “Troubleshooting 8-Port FC/GE Aggregation Card Problems,” describes the troubleshooting procedures used for 8-port FC/GE aggregation card problems.
- Chapter 7, “Troubleshooting 8-Port Multi-Service Muxponder Problems,” describes the troubleshooting procedures used for 8-port multi-service muxponder problems.
- Chapter 8, “Troubleshooting 2.5-Gbps ITU Trunk Card Problems,” describes the troubleshooting procedures used for 2.5-Gbps ITU trunk card problems.
- Chapter 9, “Troubleshooting 10-Gbps ITU Trunk Card Problems,” describes the troubleshooting procedures used for 10-Gbps ITU trunk card problems.
- Chapter 10, “Troubleshooting 10-Gbps ITU Tunable Trunk Card Problems,” describes the troubleshooting procedures used for 10-Gbps ITU tunable trunk card problems.
- Chapter 11, “Troubleshooting 10-Gbps Uplink Card Problems,” describes the troubleshooting procedures used for 10-Gbps uplink card problems.
- Chapter 12, “Troubleshooting OADM Module Problems,” describes the troubleshooting procedures used for OADM module problems.
- Chapter 13, “Troubleshooting PSM Problems,” describes the troubleshooting procedures used for PSM problems.
- Chapter 14, “Troubleshooting VOA Module Problems,” describes the troubleshooting procedures used for WB-VOA module and PB-OE module problems.
- Chapter 15, “Troubleshooting APS Problems,” describes the troubleshooting procedures used for APS problems.
- Chapter 16, “Troubleshooting OSCP Problems,” describes the troubleshooting procedures used for OSCP problems.
- Chapter 17, “Troubleshooting Threshold Alarms,” describes the troubleshooting procedures used for threshold alarm problems.
- Chapter 18, “Troubleshooting Performance History Counter Problems,” describes the troubleshooting procedures used for performance history counter problems.
- Appendix A, “Technical Support,” describes the process used to contact and provide your technical support representative with the information to resolve your problem.

Related Documentation

Use this Cisco ONS 15530 Troubleshooting Guide in conjunction with the following referenced publications:

- *Regulatory Compliance and Safety Information for the Cisco ONS 15500 Series*
Provides the regulatory compliance and safety information for the Cisco ONS 15500 Series.
- *Cisco ONS 15530 Planning Guide*
Provides detailed information on the Cisco ONS 15530 architecture and functionality.
- *Cisco ONS 15530 Hardware Installation Guide*
Provides detailed information about installing the Cisco ONS 15530.
- *Cisco ONS 15530 Optical Transport Turn-Up and Test Guide*

Provides acceptance testing procedures for Cisco ONS 15530 nodes and networks.

- *Cisco ONS 15530 Cleaning Procedures for Fiber Optic Connections*
Provides processes and procedures for cleaning the fiber optic connectors and component interfaces of the Cisco ONS 15530.
- *Cisco ONS 15530 Command Reference*
Provides commands to configure and manage the Cisco ONS 15530.
- *Cisco ONS 15530 System Alarms and Error Messages*
Describes the system alarms and error messages for the Cisco ONS 15530.
- *Cisco ONS 15530 Configuration Guide*
Describes how to configure the Cisco ONS 15530.
- *Network Management for the Cisco ONS 15530*
Provides information on the network management systems that support the Cisco ONS 15530.
- *Cisco ONS 15530 TL1 Commands*
Provides a full TL1 command and autonomous message set including parameters, AIDs, conditions and modifiers for the Cisco ONS 15530.
- *MIB Quick Reference for the Cisco ONS 15500 Series*
Describes the Management Information Base (MIB) objects and explains how to access Cisco public MIBs for the Cisco ONS 15500 Series.
- *Cisco ONS 15530 Software Upgrade Guide*
Describes how to upgrade system images and functional images on the Cisco ONS 15530.
- *Introduction to DWDM Technology*
Provides background information on the dense wavelength division multiplexing (DWDM) technology.
- *Cisco IOS Configuration Fundamentals Configuration Guide*
Provides useful information on the CLI (command-line interface) and basic shelf management.

Document Conventions

This publication uses the following conventions:

Convention	Application
boldface	Commands and keywords in body text.
<i>italic</i>	Command input that is supplied by the user.
[]	Keywords or arguments that appear within square brackets are optional.
{ x x x }	A choice of keywords (represented by x) appears in braces separated by vertical bars. The user must select one.

Convention	Application
Ctrl	The control key. For example, where Ctrl + D is written, hold down the Control key while pressing the D key.
screen font	Examples of information displayed on the screen.
boldface screen font	Examples of information that the user must enter.
< >	Command parameters that must be replaced by module-specific codes.

**Note**

Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the document.

**Caution**

Means *reader be careful*. In this situation, the user might do something that could result in equipment damage or loss of data.

**Warning****IMPORTANT SAFETY INSTRUCTIONS**

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. Statement 1071

SAVE THESE INSTRUCTIONS

Where to Find Safety and Warning Information

For safety and warning information, refer to the *Cisco Optical Transport Products Safety and Compliance Information* document that accompanied the product. This publication describes the international agency compliance and safety information for the Cisco ONS 15xxx systems. It also includes translations of the safety warnings that appear in the ONS 15xxx system documentation.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

<http://www.cisco.com/techsupport>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

The Product Documentation DVD is a comprehensive library of technical product documentation on a portable medium. The DVD enables you to access multiple versions of installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the same HTML documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .PDF versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at this URL:

<http://www.cisco.com/go/marketplace/>

Cisco Optical Networking Product Documentation CD-ROM

Optical networking-related documentation, including Cisco ONS 15xxx product documentation, is available in a CD-ROM package that ships with your product. The Optical Networking Product Documentation CD-ROM is updated periodically and may be more current than printed documentation.

Ordering Documentation

Registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

<http://www.cisco.com/go/marketplace/>

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can submit comments about Cisco documentation by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you will find information about how to:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For Emergencies only—security-alert@cisco.com

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532



Tip

We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.x through 9.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT at the aforementioned e-mail addresses or phone numbers before sending any sensitive material to find other means of encrypting the data.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>



Note

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—An existing network is down, or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of the network is impaired, while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco offerings. To order and find out more about the Cisco Product Quick Reference Guide, go to this URL:

<http://www.cisco.com/go/guide>

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:
<http://www.cisco.com/go/marketplace/>
- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:
<http://www.ciscopress.com>
- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:
<http://www.cisco.com/packet>
- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:
<http://www.cisco.com/go/iqmagazine>
or view the digital edition at this URL:
<http://ciscoiq.texterity.com/ciscoiq/sample/>
- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:
<http://www.cisco.com/ipj>
- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:
<http://www.cisco.com/en/US/products/index.html>
- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:
<http://www.cisco.com/discuss/networking>
- World-class networking training is available from Cisco. You can view current offerings at this URL:
<http://www.cisco.com/en/US/learning/index.html>



Troubleshooting Overview

This chapter gives a brief overview of the *Cisco ONS 15530 Troubleshooting Guide* as well as a troubleshooting overview of the various areas that might require troubleshooting. This chapter includes the following sections:

- 1.1 Overview, page 1-1
- 1.2 General Model of Problem Solving, page 1-2
- 1.3 Maintaining Network Information, page 1-4
- 1.4 Network and System Management, page 1-4
- 1.5 Third-Party Troubleshooting Tools, page 1-5
- 1.6 Using General Diagnostic Commands, page 1-6
- 1.7 Online Diagnostics, page 1-8
- 1.8 Configuring Online Diagnostics, page 1-9
- 1.9 Power-On Diagnostics, page 1-11
- 1.10 Checking Release Notes for Workarounds, page 1-16
- 1.11 Initial Troubleshooting Checklist, page 1-18

Basic troubleshooting processes, such as troubleshooting Ethernet connections, that are not specific to the Cisco ONS 15530 are not described in this document. This information is found online in other troubleshooting guides such as the *Cisco IOS Internetwork Troubleshooting Guide*.

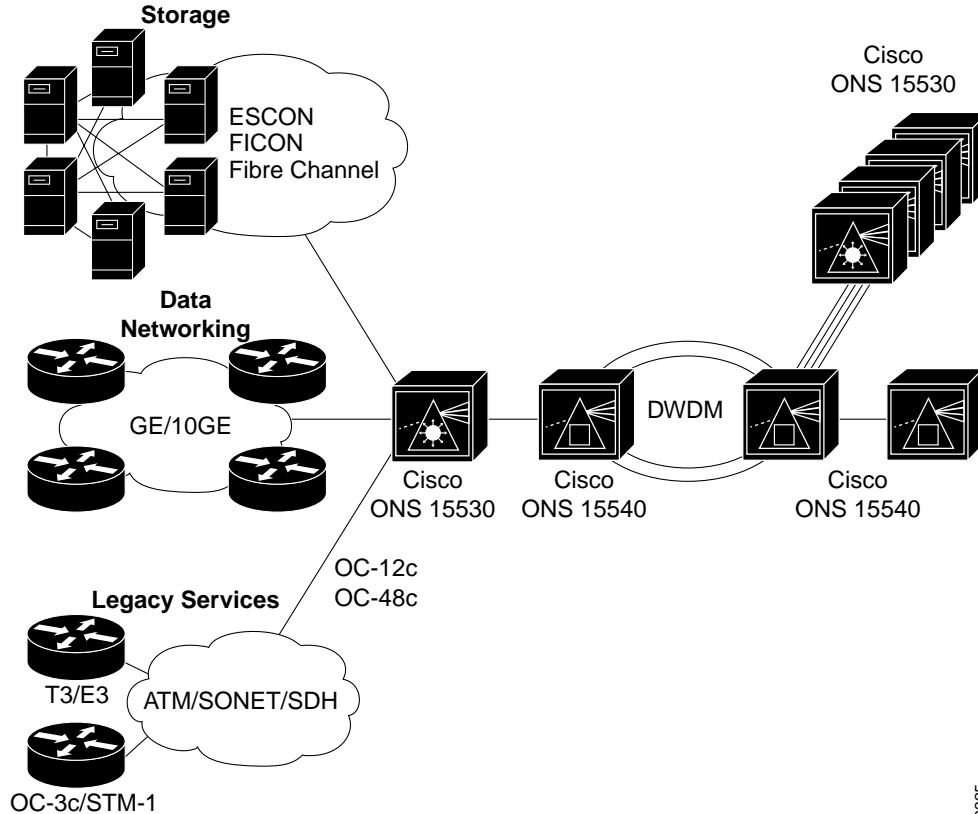
1.1 Overview

The Cisco ONS 15530 is a modular and scalable optical switching and aggregation platform designed to supplement the Cisco ONS 15540 ESP and Cisco ONS 15540 ESPx. With the Cisco ONS 15530, users can take advantage of the availability of dark fiber to build a common infrastructure that supports data, SAN (storage area network), and TDM (time-division multiplexing) traffic.

The Cisco ONS 15530 uses DWDM (dense wavelength-division multiplexing) to transport up to 32 wavelengths on a single fiber pair, and Cisco ONS 15530 systems can be stacked together for expansion and aggregation.

The Cisco ONS 15530 transports a wide variety of traffic including SONET/SDH and ATM at OC-3/STM-1, OC-12/STM-4, and OC-48/STM-16; Fast Ethernet and Gigabit Ethernet for data networking; and ESCON, Fiber Connectivity (FICON), and Fibre Channel for storage networking. Wavelengths carrying disparate traffic types can be multiplexed together onto a single fiber pair providing multiservice transport. See Figure 1-1.

Figure 1-1 Cisco ONS 15530



The flexibility of the Cisco ONS 15530 and the variety of applications it is used in can make troubleshooting system problems difficult. This guide provides information on basic troubleshooting, various troubleshooting tools and diagnostics available, and specific symptom related troubleshooting procedures.

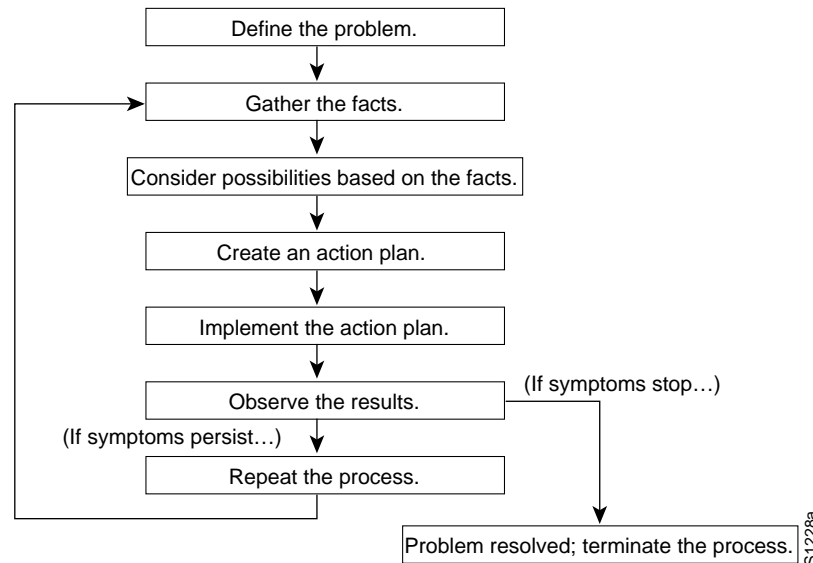
The general problem solving model, your network and system information, along with the numerous troubleshooting tools presented in this chapter, take much of the difficulty out of troubleshooting the Cisco ONS 15530.

1.2 General Model of Problem Solving

When troubleshooting the Cisco ONS 15530 in a network environment, define the specific symptoms, identify all potential problems that could be causing the symptoms, and then systematically eliminate each potential problem (from most likely to least likely) until the symptoms disappear.

Figure 1-2 illustrates the general problem-solving model. This process is not a rigid outline for troubleshooting. It is a foundation on which you can build a problem-solving process for your environment.

Figure 1-2 **General Model of Problem Solving**



The following steps detail the problem-solving process outlined in Figure 1-2:

-
- Step 1** Analyze the problem and create a clear problem statement. Define symptoms and potential causes.
 - Step 2** Gather the facts you need to help isolate possible causes.
 - Step 3** Consider possible causes based on the facts you gathered.
 - Step 4** Create an action plan based on those causes. Begin with the most likely problem and devise a plan in which you manipulate only *one* variable.
 - Step 5** Implement the action plan, performing each step carefully while testing to see whether the symptom disappears.
 - Step 6** Analyze the results to determine whether the problem is resolved.
 - Step 7** Terminate the process if the process is resolved.
 - Step 8** Create an action plan based on the next most probable cause on your list if the problem is not resolved. Return to Step 4 and repeat the process until the problem is solved.

Make sure that you undo anything you changed while implementing your action plan. Remember that you want to change only one variable at a time.



Note

If you exhaust all the common causes and actions (either those outlined in this publication or others that you have identified in your environment), contact customer service. See Appendix A, “Technical Support,” for additional information.

1.3 Maintaining Network Information

Maintaining the following details about your system configuration and network helps with troubleshooting your system:

- Maintain an accurate physical and logical map of your internetwork that outlines the physical location of all of the devices on the network and how they are connected, as well as a logical map of network addresses, network numbers, and subnetworks.
- List all network protocols implemented in your network as well as a list of the network numbers, subnetworks, zones, and areas that are associated with them.
- Note which protocols are being routed and what the correct, up-to-date configuration information is for each protocol.
- Document all the points of contact to external networks, including any connections to the Internet. For each external network connection, note what routing protocol is being used.
- Document normal network behavior and performance so that you can compare current problems with a baseline.

1.4 Network and System Management

This section describes the network management tools available for the Cisco ONS 15530. CiscoWorks 2000 supports a suit of network management applications of which the following are supported on the Cisco ONS 15530:

- 1.4.1 CiscoView
- 1.4.2 CTM
- 1.4.3 DFM

1.4.1 CiscoView

CiscoView is a device management application providing dynamic status, monitoring, and configuration information for a range of Cisco internetworking products including the Cisco ONS 15530. CiscoView displays a physical view of a device chassis, with color-coding of modules and ports for at-a-glance status. Monitoring capabilities display performance and other statistics. Configuration capabilities allow changes to devices if security privileges are granted.

Cisco ONS 15530 is supported by Embedded CiscoView and server based CiscoView. Online help for CiscoView is available for the server based CiscoView.

1.4.2 CTM

CTM (Cisco Transport Manager) is the EMS (element management system) for the Cisco ONS 15530. CTM provides standard fault, configuration, performance, and security management capabilities across the element and network management layers of the TMN (Telecommunications Management Network) reference architecture. The robust client/server-based platform easily scales to manage up to 100 simultaneous client (user) sessions and up to 1000 NEs (network elements).

1.4.3 DFM

DFM (Device Fault Manager) reports faults that occur on Cisco devices, often identifying fault conditions before users of network services realize that the condition exists. DFM analysis technology differs from the traditional rules-based approach to event analysis. DFM analysis uses a top-down approach that starts by identifying the fault conditions that affect managed systems. Because the event information necessary to diagnose fault conditions is present in the analysis model, DFM monitors only the events necessary to diagnose the condition. DFM can operate as an independent management system or can integrate with existing management applications to add fault management to the functionality already in place.

1.5 Third-Party Troubleshooting Tools

In many situations, third-party troubleshooting tools can be helpful. For example, attaching an optical analyzer to a network is less intrusive than using the **debug** commands, which are CPU switch module intensive.

Here are some typical third-party tools used for troubleshooting internetworks:

- Optical cleaning kit—Keeps your optical cable connections clean. This should be in every tool kit that has anything to do with optical equipment. Several problems you encounter will typically be associated with dirty cables.
- Optical power meter—Measures the optical power coming from and going into a piece of equipment. This is the standard operating procedure for installing and troubleshooting optical equipment. Your optical power meter must be able to measure signals at 850 nm and 1310 nm.



Note Optical power meters need to be recalibrated once per year.

- TDR (time domain reflectometer)—Locates open circuits, short circuits, crimps, kinks, sharp bends, impedance mismatches, and other defects in metallic cables. A TDR reflects a signal off the end of the cable. Opens, shorts, and other problems reflect back the signal at different amplitudes, depending on the problem. A TDR measures the time it takes for the signal to reflect and calculates the distance to a fault in the cable. TDRs can also measure the length of a cable, and some TDRs can calculate the rate of propagation based on a configured cable length.
- OTDR (optical time domain reflector/reflectometer)—Checks end-to-end loss and detects fiber breaks, splice points in the optical fiber, and fiber attenuation. This tool is essential for initial network startup and later troubleshooting fiber breaks.
- BERT (bit error rate tester)—Tests OC-3, OC-12, and OC-48 ports for end connectivity of the wavelength if the client equipment is not yet available. BERT usually has a built-in power meter to test optical power of the circuit.
- Fiber microscope—Checks the fiber interface for dirt or anything else that could degrade the optical connection.
- Patch cables—Loops back the trunk side. You should keep an assortment of multimode and single-mode patch cables with you, including 1550 nm SM trunk side cables with MU-to-SC interfaces and SC-to-SC coupler. Use attenuators as needed.
- Fixed attenuators—Adds fixed attenuation levels to connections. Five attenuators with 5 dB at 1310 nm and five with 10 dB at 1310 nm, are a good start.

- Spectrum analyzer—Views the channel spectrum or analyzes light according to wavelength. It is useful when you suspect channel cross talk and for certifying equipment and performing periodic laser tests for stability.
- Network monitors—Tracks packets crossing a network, providing an accurate picture of network activity. Network monitors do not decode the contents of frames. They are useful for creating a baseline of normal performance. Monitors collect information such as packet sizes, the number of packets, error packets, overall usage of a connection, the number of hosts and their MAC addresses, and details about communications between hosts and other devices. This data can be used to create profiles of LAN traffic and assist in locating traffic overloads, planning for network expansion, detecting intruders, and distributing traffic more efficiently.

1.6 Using General Diagnostic Commands

You can use the **show**, **debug**, **ping**, and **tracert** commands to monitor and troubleshoot your internetwork.

1.6.1 show Commands

You can use the **show** commands to perform many functions such as the following:

- Monitors the behavior of your Cisco ONS 15530 during initial installation
- Monitors normal network operation
- Isolates problem interfaces, nodes, media, or applications
- Determines when a network is congested
- Determines the status of servers, clients, or other neighbors

Table 1-1 lists some of the most commonly used **show** commands:

Table 1-1 Useful Diagnostic Commands

Command	Purpose
show interfaces <i>interface</i>	Displays statistics for the interfaces.
show controllers <i>interface</i>	Displays statistics for CPU switch module interface controllers.
show running-config	Displays the currently running configuration.
show startup-config	Displays the configuration stored in NVRAM (nonvolatile RAM).
show flash	Displays the layout and content of Flash memory.
show buffers	Displays statistics for the buffer pools on the Cisco ONS 15530.
show memory	Shows statistics about the Cisco ONS 15530 memory, including free pool statistics.
show processes	Displays information about the active processes on the Cisco ONS 15530.

Table 1-1 Useful Diagnostic Commands (continued)

Command	Purpose
show stacks	Displays information about the stack utilization of processes and interrupt routines, and the reason for the last system reboot.
show version	Displays the configuration of the system hardware, the software version, the names and sources of configuration files, and the boot images.

For more information about **show** commands, refer to the *Cisco ONS 15530 Command Reference* and the *Cisco IOS Configuration Fundamentals Command Reference* publication.

1.6.2 debug Commands

The **debug** privileged EXEC commands provide information about the traffic on (or *not* seen) on an interface, error messages generated by nodes on the network, protocol-specific diagnostic packets and cells, and other useful troubleshooting data.



Caution

Be careful when using **debug** commands. Many of these commands are CPU switch module intensive and can cause serious network problems (such as degraded performance or loss of connectivity) if they are enabled on an already heavily loaded system. When you finish using a **debug** command, remember to disable it with its specific **no debug** command (or use the **no debug all** command to turn off all debugging).

In many situations, third-party diagnostic tools can be more useful and less intrusive than using **debug** commands. See the “1.5 Third-Party Troubleshooting Tools” section on page 1-5.

1.6.3 ping Command

To check host reachability and network connectivity, use the **ping** user EXEC or privileged EXEC command. This command can be used to confirm basic network connectivity on IP networks.

For IP, the **ping** command sends ICMP (Internet Control Message Protocol) echo messages. If a station receives an ICMP echo message, it sends an ICMP echo reply message back to the source.

Using the extended command mode of the **ping** privileged EXEC command, you can specify the supported IP header options, which allow the Cisco ONS 15530 to perform a more extensive range of test options. To enter **ping** extended command mode, enter the **ping** command at the command prompt followed by a return.

To see how the command works under normal conditions, use the **ping** command when the network is functioning properly. When you are troubleshooting, you can then see the difference between normal and abnormal operation.

For detailed information about using the **ping** and extended **ping** commands, refer to the *Cisco IOS Configuration Fundamentals Command Reference* publication.

1.6.4 traceroute Command

The **traceroute** user EXEC command discovers the routes packets follow when traveling to their destinations. With the **traceroute** privileged EXEC command, the supported IP header options are specified, and the Cisco ONS 15530 can perform a more extensive range of test options.

The **traceroute** command works by using the error message generated by a Cisco ONS 15530 when a datagram exceeds its TTL (Time-To-Live) value. First, probe datagrams are sent with a TTL value of one. This causes the first Cisco ONS 15530 to discard the probe datagrams and send back `time exceeded` error messages. The **traceroute** command then sends several probes, and displays the round-trip time for each. After every third probe, the TTL increases by one.

Each outgoing packet can result in one of two error messages. A `time exceeded` error message indicates that an intermediate Cisco ONS 15530 has seen and discarded the probe. A `port unreachable` error message indicates that the destination node has received the probe and discarded it because it could not deliver the packet to an application. If the timer goes off before a response comes in, the **traceroute** command displays an asterisk (*).

The **traceroute** command terminates when the destination responds, when the maximum TTL is exceeded, or when the user interrupts the **traceroute** command with the escape sequence.

To see how the command works under normal conditions, use the **traceroute** command when the network is functioning properly. When you are troubleshooting, you can then see the difference between normal and abnormal operation.

For detailed information about using the **traceroute** command, refer to the *Cisco ONS 15530 Configuration Guide*. For additional information on using **debug** commands refer to the *Cisco IOS Debug Command Reference*.

1.7 Online Diagnostics

This section describes the online diagnostics available for troubleshooting your Cisco ONS 15530. Online diagnostics provide the following types of tests:

- Accessibility tests between the CPU switch module and the modules.
- OIR (online insertion and removal) diagnostic tests.

The Cisco ONS 15530 displays an error message on the console when it detects a hardware failure or problem.



Note

Online diagnostic tests only run on the active CPU switch module.

1.7.1 Accessibility Test

The accessibility tests ensure connectivity, at a configurable interval, between the following:

- OADM modules
- Transponder line cards
- Carrier motherboards
- Active CPU switch module
- Standby CPU switch module, if it is present

- 2.5-Gbps ITU trunk cards
- 10-Gbps ITU trunk cards
- 10-Gbps ITU tunable trunk cards
- 10-Gbps uplink cards
- ESCON aggregation cards
- 8-port FC/GE aggregation cards

1.7.2 OIR Test

OIR tests check the functioning of the CPU switch module and interfaces on a per-port basis. The CPU switch module performs these tests when the system boots up and when you insert a module or motherboard into a slot. The OIR test sends a packet to the interface loopback and expects to receive it within a certain time period. If the packet does not reach the port within the expected time period, or the received packet is corrupted, an error is registered and the port is changed to an administratively down state. Packets that are 1000 bytes in size are used in the test.

1.8 Configuring Online Diagnostics

To configure online diagnostics, use the following global configuration commands:

Command	Purpose
<code>[no] diag online</code>	Enables or disables online diagnostic tests on all components on the shelf.
<code>[no] diag online slot <i>slot</i></code>	Enables or disables online diagnostic tests only on the components in a chassis slot.
<code>[no] diag online subslot <i>slot/subcard</i></code>	Enables or disables online diagnostic tests only on the components in a chassis subslot.
<code>[no] debug diag online [background online-insertion-removal redundancy]</code>	Enables debugging of online diagnostic tests.

Examples

The following example shows how to enable all online diagnostic tests:

```
Switch# diag online
```

The following example shows how to enable online diagnostic tests for the components in slot 3:

```
Switch# diag online slot 3
```

The following example shows how to enable debugging for online diagnostics:

```
Switch# debug diag online
```

1.8.1 Displaying the Online Diagnostics Configuration and Results

To display the online diagnostics configuration and results, use the following EXEC command:

Command	Purpose
<code>show diag online [[detail oir] slot slot]</code>	Displays information about the online diagnostic tests and the test results.

Example

The following example shows how to display detailed access test information:

```
Switch# show diag online
-----
Online Diagnostics Current Summary Information
-----
On ACTIVE CPU card Slot: 5
CPU Uptime: 1d02h

Slot          CardType          Enabled    Bootup/
              15530-CPU=        Yes        Disabled
              15530-CPU=        Yes        Disabled
              15530-CPU=        Yes        Disabled
              15530-CPU=        Yes        Disabled

Periodic      Previous
Background    Failures
tests         tests

-----
0/ 0/* PROTO-HAMPTONS-MUX    Yes Disabled    Pass    No
0/ 1/* PROTO-HAMPTONS-MUX    Yes Disabled    Pass    No
5/*/*          15530-CPU=        Yes Disabled    Pass    No
6/*/*          15530-CPU=        Yes Disabled    Pass    No
```

Example

The following example shows how to display diagnostic test status and details:

```
Switch# show diag online details
-----
Online Diagnostics was DISABLED at 0 minutes
This information is the LAST status before disabling
Specific Slots maybe configured as enabled
-----

Online Diagnostics Detailed Information
-----
On ACTIVE CPU card Slot: 5
CPU Uptime: 1 day, 1 hour, 8 minutes

Slot[0]

Online Insertion Tests
Slot          CardType          TestType    Status    LastRunTime    LastFailTime
-----
0/ 0/* PROTO-HAMPTONS-MUX    idpromAcc  Disabled    nev          nev
0/ 1/* PROTO-HAMPTONS-MUX    idpromAcc  Disabled    nev          nev

Online Background Tests
Slot          CardType          TestType    Status    LastRunTime    LastFailTime
-----
0/ 0/* PROTO-HAMPTONS-MUX    idpromAcc  Disabled    nev          nev
0/ 1/* PROTO-HAMPTONS-MUX    idpromAcc  Disabled    nev          nev
```

```

Slot [5]

Online Insertion Tests
Slot          CardType          TestType      Status      LastRunTime  LastFailTime
~~~~~        ~~~~~
5/*/*        15530-CPU=    srcStatus    Disabled    nev          nev
              IdpromAcc     Disabled

Online Background Tests
Slot          CardType          TestType      Status      LastRunTime  LastFailTime
~~~~~        ~~~~~
5/*/*        15530-CPU=    srcStatus    Disabled    nev          nev
              IdpromAcc     Disabled

Slot [6]

Online Insertion Tests
Slot          CardType          TestType      Status      LastRunTime  LastFailTime
~~~~~        ~~~~~
6/*/*        15530-CPU=    srcStatus    Disabled    nev          nev
              IdpromAcc     Disabled

Online Background Tests
Slot          CardType          TestType      Status      LastRunTime  LastFailTime
~~~~~        ~~~~~
6/*/*        15530-CPU=    srcStatus    Disabled    nev          nev
              IdpromAcc     Disabled

```

1.9 Power-On Diagnostics

Power-on diagnostics test the accessibility and basic functionality of the components and isolates the faults to FRU level on the Cisco ONS15530. All power-on diagnostic tests are enabled by default. All power-on diagnostic tests can be disabled and monitored by using the following commands.



Note

All the power-on diagnostic tests will be run from the primary CPU switch module. Only CPU switch module related and basic line card access tests are done from the secondary CPU switch module. Power-on diagnostic test results will be displayed for the cards which are present at the time of system bootup. Any removal or insertion of cards will not change the output of this command.

1.9.1 Configuring Power-On Diagnostics

All power-on diagnostic tests are enabled by default. To enable the power-on diagnostic tests, use the following global configuration commands in configuration mode, use the **no** form of the command to disable the power-on diagnostic tests:

Command	Purpose
[no] diag power-on	Enables or disables power-on diagnostic tests on all components on the shelf.
[no] diag power-on 2gfc	Enables or disables power-on diagnostic tests for 4-port 1-Gbps/2-Gbps FC aggregation cards.

Command	Purpose
[no] diag power-on carrier-mb <i>slot-number</i>	Enables or disables power-on diagnostic tests for carrier motherboards.
[no] diag power-on cpu	Enables or disables power-on diagnostic tests for CPU switch modules.
[no] diag power-on escon-10p	Enables or disables power-on diagnostic tests for the 10-port ESCON multiplexing line card.
[no] diag power-on fcge-8p	Enables or disables power-on diagnostic tests for the 8-port FC/GE aggregation card.
[no] diag power-on itu2	Enables or disables power-on diagnostic tests for the 10-Gbps ITU trunk card.
[no] diag power-on itu2-tun	Enables or disables power-on diagnostic tests for the 10-Gbps ITU tunable trunk card.
[no] diag power-on itu3	Enables or disables power-on diagnostic tests for the 2.5-Gbps ITU trunk card.
[no] diag power-on mdx idprom subslot	Enables or disables power-on diagnostic tests for the OADM modules.
[no] diag power-on oscm	Enables or disables power-on diagnostic tests for the OSC modules.
[no] diag power-on psm	Enables or disables power-on diagnostic tests for the PSM.
[no] diag power-on tsp1	Enables or disables power-on diagnostic tests for the transponder line cards.
[no] diag power-on voa	Enables or disables power-on diagnostic tests for the VOA modules.
show diag power-on	Displays the power-on diagnostic tests results for the entire system or a specific slot.

Example

The following example shows how to enable all power-on diagnostic tests:

```
Switch(config)# diag power-on
```

Refer to the *Cisco ONS 15530 Command Reference* for more information on the power-on diagnostic commands.

1.9.2 Displaying the Power-On Diagnostic Test Results

To display the power-on diagnostic test results, use the following EXEC command:

Command	Purpose
show diag power-on	Displays the summarized power-on diagnostic results.

Command	Purpose
<code>show diag power-on detail</code>	Displays the results of the power-on diagnostic tests for the entire system.
<code>show diag power-on slot [slot]</code>	Displays the results of the power-on diagnostic tests for the specified slot.

Example

The following example shows how to display the summarized power-on diagnostic results.

```
Switch# show diag power-on
-----
Power-on Diagnostics: Version 1.0
System-wide result: PASSED
Ran on: Mon Mar 13 2000      At: 03:45:13 UTC      CPU was: Primary
-----

Slot/Subslot  Card-type      Result
-----
0/1           mdx            Passed
1/*          tsp1          Passed
3/*          itu2          Passed
4/*          tsp1          Passed
6/*          cpu           Passed
7/*          tsp1          Passed
8/*          carrier-mb    Passed
8/0          oscm          Passed
8/1          oscm          Passed
9/*          escon-10p     Passed
10/*         tsp1          Passed
```

Example

The following example shows how to display detailed access test information:

```
Switch# show diag power-on detail
-----
Power-on Diagnostics: Version 1.0
System-wide result: FAILED
Ran on: Mon Mar 13 2000      At: 03:45:13 UTC      CPU was: Primary
-----

Subslot: 0/1      mdx            Result: Passed
H/w Ver: 1.0      FPGA func ver: N/A      Versions compatible: N/A

Test-name          Result      Cause-code
-----
idprom            Passed      -
-----

Slot: 1/*          tsp1          Result: Passed
H/w Ver: 5.10      FPGA func ver: 3.12      Versions compatible: Yes

Test-name          Result      Cause-code
-----
jtag-access        Passed      -
lrc-access         Passed      -
backplane-eth-lb   Passed      -
aps-msg-int-bus    Passed      -
hudjr-access       Passed      -
hudjr-ingress-inter Passed      -
hudjr-ingress-serde Passed      -
hudjr-egress-intern Passed      -
```

1.9.2 Displaying the Power-On Diagnostic Test Results

```

hudjr-egress-serdes      Passed      -
-----
Slot: 3/*                itu2                                Result: Passed
H/w Ver: 4.9             FPGA func ver: 2.31             Versions compatible: Yes

Test-name                Result      Cause-code
-----
jtag-access              Passed      -
lrc-access                Passed      -
backplane-eth-lb         Passed      -
aps-msg-int-bus          Passed      -
component-access         Passed      -
sii-memory                Passed      -
qphy-fabric-lb           Passed      -
om-fifo                   Passed      -
-----
Slot: 4/*                tsp1                                Result: Passed
H/w Ver: 5.8             FPGA func ver: 3.12             Versions compatible: Yes

Test-name                Result      Cause-code
-----
jtag-access              Passed      -
lrc-access                Passed      -
backplane-eth-lb         Passed      -
aps-msg-int-bus          Passed      -
hudjr-access              Passed      -
hudjr-ingress-inter      Passed      -
hudjr-ingress-serde      Passed      -
hudjr-egress-intern      Passed      -
hudjr-egress-serdes      Passed      -
-----
Slot: 6/*                cpu                                Result: FAILED
H/w Ver: 4.6             FPGA func ver: 1.43             Versions compatible: Yes

Test-name                Result      Cause-code
-----
cpu-l1-cache             Passed      -
cpu-l2-cache             Passed      -
gt-pci0                   Passed      -
iofpga-access            Passed      -
nvrn                      Passed      -
system-tod                Passed      -
bootflash                 Passed      -
src-access                Passed      -
src-timer                 Passed      -
sw-fabric-config          Passed      -
bcom-sw-access            Passed      -
bcom-sw-config            Passed      -
gt-mii0-internal-lb      Passed      -
gt-mii1-internal-lb      Passed      -
gt-mpsc-internal-lb      Passed      -
bp-idprom-test            FAILED      1
power-supply0             FAILED      3
power-supply1             Passed      -
temp-sensor                Passed      -
gt-interrupt              Passed      -
interrupt0                 Passed      -
interrupt2                 Passed      -
interrupt3                 Passed      -
interrupt7                 Passed      -
interrupt8                 Passed      -
-----
Slot: 7/*                tsp1                                Result: Passed
H/w Ver: 5.8             FPGA func ver: 3.12             Versions compatible: Yes

```

```

Test-name          Result          Cause-code
~~~~~
jtag-access        Passed          -
lrc-access         Passed          -
backplane-eth-lb   Passed          -
aps-msg-int-bus    Passed          -
hudjr-access       Passed          -
hudjr-ingress-inter Passed          -
hudjr-ingress-serde Passed          -
hudjr-egress-intern Passed          -
hudjr-egress-serdes Passed          -
-----
Slot: 8/*          carrier-mb          Result: Passed
H/w Ver: 4.2       FPGA func ver: 1.37 Versions compatible: Yes

Test-name          Result          Cause-code
~~~~~
jtag-access        Passed          -
lrc-access         Passed          -
backplane-eth-lb   Passed          -
aps-msg-int-bus    Passed          -
-----
Subslot: 8/0       oscm              Result: Passed

Test-name          Result          Cause-code
~~~~~
hudjr-access       Passed          -
idprom            Passed          -
hudjr-internal-lb Passed          -
serdes-lb         Passed          -
-----
Subslot: 8/1       oscm              Result: Passed

Test-name          Result          Cause-code
~~~~~
hudjr-access       Passed          -
idprom            Passed          -
hudjr-internal-lb Passed          -
serdes-lb         Passed          -
-----
Slot: 9/*          escon-10p          Result: Passed
H/w Ver: 3.4       FPGA func ver: 2.36 Versions compatible: Yes

Test-name          Result          Cause-code
~~~~~
jtag-access        Passed          -
lrc-access         Passed          -
backplane-eth-lb   Passed          -
aps-msg-int-bus    Passed          -
component-access   Passed          -
encap-lb           Passed          -
qphy-lb            Passed          -
fabric-lb          Passed          -
-----
Slot: 10/*         tsp1              Result: Passed
H/w Ver: 5.9       FPGA func ver: 3.12 Versions compatible: Yes

Test-name          Result          Cause-code
~~~~~
jtag-access        Passed          -
lrc-access         Passed          -
backplane-eth-lb   Passed          -
aps-msg-int-bus    Passed          -

```

```

hudjr-access          Passed          -
hudjr-ingress-inter   Passed          -
hudjr-ingress-serde   Passed          -
hudjr-egress-intern   Passed          -
hudjr-egress-serdes   Passed          -

```

Example

The following example shows how to display detailed test information for a specific slot:

```

Switch# show diag power-on slot 5
Power-on Diagnostics:Version 1.0
System-wide result:Passed
Ran on:Fri Dec 13 2002          At:22:29:11 UTC          CPU was:Primary

```

```

-----
Slot:5/*          cpu          Result:
Passed
H/w Ver:6.1          FPGA func ver:1.43          Versions compatible:Yes

```

```

Test-name          Result          Cause-code
-----
cpu-l1-cache       Passed          -
cpu-l2-cache       Passed          -
gt-pci0            Passed          -
iofpga-access      Passed          -
nvram              Passed          -
system-tod         Passed          -
bootflash          Passed          -
src-access         Passed          -
src-timer          Passed          -
sw-fabric-config   Passed          -
bcom-sw-access     Passed          -
bcom-sw-config     Passed          -
gt-mii0-internal-lb Passed          -
gt-mii1-internal-lb Passed          -
gt-mpsc-internal-lb Passed          -
bp-idprom-test     Passed          -
power-supply0      Passed          -
power-supply1      N/A            -
temp-sensor        Passed          -
gt-interrupt       Passed          -
interrupt0         Passed          -
interrupt2         Passed          -
interrupt3         Passed          -
interrupt7         Passed          -
interrupt8         Passed          -

```

1.10 Checking Release Notes for Workarounds

There are two methods you can use to check for Cisco IOS software bugs (defect tracking tool numbers [DDTs]) in your version of the Cisco IOS software. You can use the Bug Navigator II or check the release notes. Often, your problems with the Cisco ONS 15530 have been fixed or a workaround has been determined in a more recent version of software.

1.10.1 Using Bug Toolkit

Bug Toolkit is a tool to search for known bugs based on software version, feature set, and keywords. The resulting matrix shows when each bug was integrated, or fixed if applicable.

You can access Bug Navigator II on the World Wide Web at http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl. Then follow these steps:

-
- Step 1** Enter your user name and password at the login prompt if you are not already logged in to Cisco.com.
 - Step 2** Read the Bug Navigator II Help instructions.
 - Step 3** Select your hardware from the Cisco Hardware list. The Bug Navigator search tool replaces Bug Navigator II Help (in the right frame of the page).
 - Step 4** Select the following from the drop-down menus:
 - Version
 - Revision
 - Severity



Note As an option, you can enter words or phrases (separated by commas) in the data entry field to limit your search.

- Step 5** Click the **Search** button.

The entire window is replaced with a Bug Search Results window with a list of DDTS containing your search criteria. Look at the Bug reports listed in the titles column. An existing bug entry that describes the problem you are having may have been fixed in a more recent version of the Cisco IOS software. Look in the Fixed-in column for a later version of the Cisco IOS software. All you might have to do to solve your problem is upgrade your software.

If a software upgrade is not listed as a way to solve your problem, double-click on the bug title and read the DDTS details; a workaround might be listed there.

1.10.2 Checking Cisco IOS Release Notes

Release notes describe the features and caveats for Cisco IOS software releases. The release notes are listed by both product and Cisco IOS release number.

The “Caveats” section of the release notes lists known caveats by tracking the DDTS number and the release number, and indicates whether the caveat has been corrected.

The “Caveat Symptoms and Workarounds” section summarizes caveat symptoms and suggested workarounds. You can also search through this section online, using either a word string or the DDTS number.

1.11 Initial Troubleshooting Checklist

Before you start the troubleshooting process, confirm that the network and client connections were designed correctly using the information in the *Cisco ONS 15530 Planning Guide* and the interfaces were configured correctly using the information in the *Cisco ONS 15530 Configuration Guide* and the *Cisco ONS 15530 Command Reference*.

Next confirm the integrity of the hardware and its installation by performing the following:

- Reseat the cable.
- Clean the cable, connectors, couplers, and attenuators.
- Confirm that the Tx and Rx fiber optic connections are not mixed.
- Confirm all modules and motherboards are completely seated and the captive screws are tightened securely to completely mate the optical fiber connectors to the backplane.
- Check the signal level at each input and output to check for too much or too little attenuation.
- Verify that all line cards, modules, and carrier motherboards are properly seated in the slots.



Troubleshooting CPU Switch Module Problems

This chapter describes how to troubleshoot CPU switch module problems. This chapter includes the following sections:

- 2.1 Overview, page 2-1
- 2.2 Initial Troubleshooting Checklist, page 2-2
- 2.3 Verifying CPU Switch Module Configuration, page 2-2
- 2.4 Recovering a Lost Password, page 2-4
- 2.5 Verifying NME Interface Configurations, page 2-5
- 2.6 Troubleshooting CPU Switch Module Memory, page 2-9
- 2.7 Verifying Hardware and Software Versions, page 2-9
- 2.8 Verifying Hardware and Software Compatibility, page 2-13
- 2.9 Troubleshooting Redundant CPU Switch Modules, page 2-15
- 2.10 Troubleshooting CPU Switch Module Problems, page 2-22

2.1 Overview

The Cisco ONS 15530 supports two CPU switch modules for redundancy, one in active mode and the other in hot-standby mode. CPU switch modules are installed in slot 5 and slot 6. Each CPU switch module has a processor, a switch fabric, a clock, an Ethernet switch for communication between CPU switch modules and with the LRC (line card redundancy controller) on the OADM modules and line cards, and an SRC (switch card redundancy controller). The active CPU switch module controls the system. All LRCs in the system use the system clock and synchronization signals from the active CPU switch module. Interfaces on the CPU switch modules permit access by 10/100 Ethernet, console terminal, or modem connections.



Note

For information on slot assignments, CPU switch module LEDs, alarm condition clear and reset button, interrupt clear and reset button, NME LEDs, and cabling, refer to the *Cisco ONS 15530 Hardware Installation Guide*. For default configuration of the various modules, refer to the *Cisco ONS 15530 Configuration Guide* and the *Cisco ONS 15530 Command Reference*.

2.2 Initial Troubleshooting Checklist

Follow this initial checklist before proceeding with the troubleshooting procedures:

- Issue the **show running-config** command to check the running configuration.
- Ensure the LEDs on the CPU switch modules show the proper state.
- Ensure the Ethernet and Console cables are connected properly.
- Issue the **show facility-alarm status** command to check for CPU switch module, fan, or power supply alarms.
- Issue the **show hardware detail** command to verify the CPU switch module functional image.
- Ensure online and power-on diagnostics do not report any alarms or failures for the CPU switch module.
- Ensure the active and standby CPU switch modules are compatible.
- Ensure the active and standby CPU switch module have same version of software installed.

2.3 Verifying CPU Switch Module Configuration

To display the CPU switch module configuration and status, issue the **show running-config** command.

Command	Purpose
show running-config	Shows all components of the CPU switch module running a configuration.

The following example shows the **show running-config** command, which displays all the components of the CPU switch module configuration. For a detailed description of this command, refer to the *Cisco IOS Configuration Fundamentals Command Reference*.

```
Switch# show running-config
Building configuration...

Current configuration : 2971 bytes
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service internal
!
hostname top
!
boot system bootflash:ons15530-i-mz.sar-f-rep
boot bootldr bootflash:ons15530-i-mz.sar-f-rep
logging snmp-authfail
logging queue-limit 100
logging buffered 10000 debugging
enable password
!
diag online
no diag power-on
```



```
ip subnet-zero
ip ftp source-interface FastEthernet0
ip ftp username
ip ftp password
no ip domain-lookup
!
!
!
<information deleted>

control-plane
!
!
redundancy
  associate group sp
    aps working Wavepatch4/0/0
    aps protection Wavepatch4/0/1
    aps enable
  standby privilege-mode enable
!
!
interface Loopback0
  no ip address
!
interface FastEthernet0
  ip address 172.25.22.125 255.255.255.0
  duplex auto
  speed auto
  no cdp enable
!
interface Fastethernet-sby0
  no ip address
  shutdown
  duplex auto
  speed auto
!
<information deleted>
!
router ospf 100
  log-adjacency-changes
  redistribute connected subnets
  redistribute static subnets
!
ip classless
ip route 0.0.0.0 0.0.0.0 FastEthernet0
ip route 172.25.18.0 255.255.255.0 FastEthernet0
no ip http server
!
!
!
snmp-server engineID local 80000009030000016447A1D1
snmp-server community public RW
snmp-server location san-jose-dev-test
snmp-server contact Edward.Ding : eding@cisco.com
snmp-server enable traps snmp authentication warmstart
snmp-server enable traps tty
snmp-server enable traps bgp
snmp-server enable traps oscp
snmp-server enable traps config
snmp-server enable traps syslog
snmp-server enable traps entity
snmp-server enable traps fru-ctrl
snmp-server enable traps topology throttle-interval 60
snmp-server enable traps rf
```

```

snmp-server enable traps aps
snmp-server enable traps patch
snmp-server enable traps alarms
banner motd ^C
*****^C
alias associate-group g400 ag400
!
line con 0
  exec-timeout 0 0
line aux 0
line vty 0 4
  exec-timeout 0 0
  password lab
  login
  length 0
  width 0
!
exception core-file /tftpboot/eding/CORE/h3
exception protocol ftp
exception dump 172.20.46.50
end

```

2.4 Recovering a Lost Password

This section describes the procedure to recover a lost login or to enable a password. The procedure differs depending on the platform and the software used, but in all cases, password recovery requires that the system be taken out of operation and powered down.

If you need to perform the following procedure, make certain that there are secondary systems that can temporarily serve the functions of the system undergoing the procedure. If this is not possible, advise all potential users and, if possible, perform the procedure during low-use hours.



Note

Make a note of your password, and store it in a secure place.

All of the procedures for recovering lost passwords depend on changing the configuration register of the system. This is done by reconfiguring the system software.

More recent Cisco platforms run from Flash memory or are netbooted from a network server and can ignore the contents of NVRAM (nonvolatile random-access memory) when booting. By ignoring the contents of NVRAM, you can bypass the configuration file (which contains the passwords) and gain complete access to the system. You can then recover the lost password or configure a new one.



Note

If your password is encrypted, you cannot recover it. You must configure a new password.

Follow these steps to recover a password:

-
- Step 1** Enter the **show version** command and the configuration register value in the privileged EXEC mode. The default value is 0x2102.
 - Step 2** Power up the Cisco ONS 15530.

- Step 3** Press the **Break** key sequence or send a break signal, which is usually `^]` within 60 seconds of turning the system on. If you do not see the `>` prompt with a system name, the terminal is not sending the correct break signal. In that case, check the terminal or terminal emulation setup.
- Step 4** Enter the **confreg** command at the `>` prompt.
- Step 5** Answer **yes** to the `Do you wish to change configuration [y/n]?` prompt.
- Step 6** Answer **no** to all the questions that appear until you reach the `Ignore system config info [y/n]` prompt. Answer **yes**.
- Step 7** Answer **no** to the remaining questions until you reach the `Change boot characteristics [y/n]?` prompt. Answer **yes**.
- Step 8** Enter **2** at the `enter to boot:` prompt.
- Step 9** Answer **no** to the `Do you wish to change configuration [y/n]?` prompt.
- Step 10** Enter the **reset** command at the `rommon>` prompt.
- Step 11** Enter the **enable** command at the `switch>` prompt. You are in enable mode and see the `switch#` prompt.
- Step 12** Enter the **show startup-config** command to view your password.
- Step 13** Proceed to Step 16 if your password is clear text. Or, continue with Step 14 if your password is encrypted.
- Step 14** Enter the **configure memory** command to copy the NVRAM into memory if your password is encrypted.
- Step 15** Enter the **copy running-config startup-config** command.
- Step 16** Enter the **configure terminal** command.
- Step 17** Enter the **enable secret password** command.
- Step 18** Enter the **config-register value** command, where *value* is whatever value you entered in Step 1.
- Step 19** Enter the **exit** command to exit configuration mode.
- Step 20** Enter the **copy running-config startup-config** command.
- Step 21** Enter the **reload** command at the prompt.
-

2.5 Verifying NME Interface Configurations

The administration interfaces provide simple command-line interfaces to all internal management and debugging facilities of the CPU switch module. To manage and debug the CPU switch module, you can use the NME (network management Ethernet) interface, the console port, and the auxiliary port.

For cable connection information for each of these interface ports, refer to the *Cisco ONS 15530 Hardware Installation Guide*. For initial configuration information, refer to the *Cisco ONS 15530 Configuration Guide* and the *Cisco ONS 15530 Command Reference*.

The NME interface has a full duplex, auto sensing connection with troubleshooting LEDs on the CPU switch module faceplate.

You can configure and monitor the NME connection using the CLI. The NME connection appears in the configuration as FastEthernet 0 or FastEthernet-sby 0 depending on the slot where the CPU switch module is installed.

To display the NME FastEthernet module configuration and status, use the following commands:

Command	Purpose
<code>show interfaces FastEthernet 0</code>	Displays the status of the physical interface.
<code>show controllers</code>	Displays the interface memory management and error counters on the FastEthernet interface.

Follow these steps to verify the NME interface:

Step 1 Issue the `show interfaces FastEthernet 0 slot/subcard/port` command to check the NME interface configuration.

```
Switch# show interfaces FastEthernet 0
→ FastEthernet0 is up, line protocol is up
   Hardware is Gt96k FE, address is 0009.7c1a.cb50 (bia 0009.7c1a.cb50)
   Internet address is 172.25.22.125/24
   MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
   Encapsulation ARPA, loopback not set
   Keepalive set (10 sec)
→ Half-duplex, 100Mb/s, 100BaseTX/FX
   ARP type: ARPA, ARP Timeout 04:00:00
→ Last input 00:00:00, output 00:00:06, output hang never
   Last clearing of "show interface" counters never
   Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
   Queueing strategy: fifo
   Output queue: 0/40 (size/max)
   5 minute input rate 3000 bits/sec, 5 packets/sec
   5 minute output rate 0 bits/sec, 0 packets/sec
     131803 packets input, 8271274 bytes
       Received 131333 broadcasts (0 IP multicast)
         0 runts, 0 giants, 0 throttles
→  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog
     0 input packets with dribble condition detected
       3254 packets output, 200502 bytes, 0 underruns
→  0 output errors, 0 collisions, 2 interface resets
→  0 babbles, 0 late collision, 0 deferred
→  0 lost carrier, 0 no carrier
→  0 output buffer failures, 0 output buffers swapped out
```

Step 2 Check the FastEthernet field to see whether the interface is up. If it is down, check for the following:

- Disconnected or faulty cabling. Check cables.
- Hardware failure. Swap hardware.

If administratively down, the interface has been administratively taken down. Issue the `no shutdown` interface configuration command to reenab the interface.

Step 3 Check the line protocol field to see whether the status is up.

If the interface is down, the line protocol software processes might have determined that the line is unusable or the local or remote interface might be misconfigured. See if the interface can be brought up by following the recommendations in Step 2.

Step 4 Check the duplex mode field. It should match the speed of the interface and be configured as auto-negotiation.

- Step 5** Check the last input and last output fields. They show the number of hours, minutes, and seconds since the last packet was successfully received or transmitted by the interface.
- Step 6** Check the output hang field. It shows the number of hours, minutes, and seconds since the last reset caused by a lengthy transmission.
- Step 7** Check the CRC field. The presence of many CRC errors, but not many collisions, indicates excessive noise. If the number of errors is too high, check the cables for damage. If you are using UTP cable, make sure you are using Category 5 cables and not another type, such as Category 3.



Note Errors and the input and output difference should not exceed 0.5 to 2.0 percent of traffic on the interface.

- Step 8** Check the collisions fields. These numbers indicate packet collisions and these numbers should be very low. The total number of collisions, with respect to the total number of output packets, should be 0.1 percent or less.
- Step 9** Check the late collisions fields. Late collisions should never occur in a properly designed Ethernet network. They usually occur when Ethernet cables are too long or when there are too many repeaters in the network.
- Step 10** Check carrier fields. These numbers indicate a lost carrier detect signal and can be caused by a malfunctioning interface that is not supplying the transmit clock signal or by a cable problem. If the system notices that the carrier detect line of an interface is up, but the line protocol is down, it periodically resets the interface in an effort to restart it. Interface resets can also occur when an interface is looped back or shut down.
- Step 11** Check the buffer fields. These numbers indicate the number of received packets discarded because there was no buffer space. Broadcast storms on Ethernet networks, and bursts of noise on serial lines, are often responsible for no-input buffer events.
- Step 12** Check the FastEthernet field to see whether the interface is up. If it is down, see if the interface can be brought up by following the recommendations in Step 2. If administratively down, the interface has been administratively taken down. Issue the **no shutdown** interface configuration command to reenab the interface.

If you determine that the connection is configured incorrectly, refer to the *Cisco ONS 15530 Configuration Guide*.

In addition, you can use the **show controllers** command to troubleshoot the status of the NME interface configuration:

```
Switch# show controllers fastethernet 0
Interface FastEthernet0
Hardware is GT96K FE ADDR: 62118CA0, FASTSEND: 0, MCI_INDEX: 0
DIST ROUTE ENABLED: 0
Route Cache Flag: 1
GPIO 2 CONF= 7FFF7FFF
GPIO 2 IO= 3D003D
CIU arbit = 2A8
PHY add register = 0x3E0
PHY data register = 0xF1F003A
Port Configuration Register= 0x80
    ENABLE HT8K HMOD0
Port Configuration Extend Register= 0xCD00
    TX1:1 RXPRI=DE(00) ~FLCNTL ~FLNKP MFL64KB E
Port Command Register= 0x0
Port Status Register= 0x9
```

2.5 Verifying NME Interface Configurations

```

100MB HDPX FCTL EN LNK UP ~PAUSED TX oFF
Serial Parameter Register= 0x218823
Hash table pointer= 0x35A83C0
Source ADDR L= 0x0
Source ADDR H= 0x0
SDMA configuration register= 0x2200
    RETX 0 RX BE TX BE FRINT BSIZE 4
SDMA command register= 0x1000080
    SRT TXL EN RX
Interrupt MASK= 0x80003DCD
Interrupt Cause= 0x0

Serial 0 mask 3
Serial 0 cause 0
IP DIFFSERV P0L= 0x0 IP DIFFSERV P0H= 0x0
IP DIFFSERV P1L= 0x0 IP DIFFSERV P1H= 0x0
IP VLAN TAG PRI= 0xF0CC
IP VLAN TAG PRI= 0xF0CC
First rxd Q0= 0x35E85A0 Curr rxd Q0= 0x35E85A0
First rxd Q1= 0x35E88A0 Curr rxd Q1= 0x35E88A0
First rxd Q2= 0x35E8D00 Curr rxd Q2= 0x35E8D00
First rxd Q3= 0x35E9160 Curr rxd Q3= 0x35E9160
First txd Q0= 0x35E99D0 First txd Q1= 0x35E9E00

gt96kfe_instance=0x6211AA58, registers=0xB4088800
rx ring entries=64, tx ring entries=128
rxring0=0x35E8440, rxring1=0x35E88A0, rxring2=0x35E8D00, rxring3=0x35E9160
malloc rxring0=0x35E8440, rxring1=0x35E88A0, rxring2=0x35E8D00, rxring3=0x35E91
60
Head rxring0=0xD, rxring1=0x0, rxring2=0x0, rxring3=0x0
Tail rxring0=0x0, rxring1=0x0, rxring2=0x0, rxring3=0x0
Shadow rxring0=0x6211ACE0, rxring1=0x6211AE20, rxring2=0x6211AF60, rxring3=0x62
125CA0
tx_limited=0(128)
txring0=0x35E95C0, txring1=0x35E9E00
Head txring0=0x41, txring1=0x0
Tail txring0=0x41, txring1=0x0
Tail COUNT txring0=0x0, txring1=0x0

PHY registers:

Register 0x00: 1000 782D 0040 6212 01E1 40A1 0003 0000
Register 0x08:
Register 0x10: D000 0301 0000 0000 0000 017F 0100 0000
Register 0x18: 003A F33E 8F00 FF00 002A C000 20A0

MIB counters:

bytes_rcvd          =11564162
bytes_sent          =214232
frames_rcvd         =156732
frames_sent         =3265
total_bytes_rcvd    =11564162
total_frames_rcvd   =156735
bcast_frames_rcvd   =131833
mcast_frames_rcvd   =22545
crc_errors          =0
ovr_sized_frames    =0
fragments           =3
jabber              =0
collision           =0
late_collision      =0
64bytes_frames      =146311
65_127bytes_frames =8619

```

```

128_255bytes_frames      =1015
256_511bytes_frames      =4056
512_1023bytes_frames     =0
1023_maxbytes_frames     =0
rx_error                 =0
dropped_frames           =0
mcast_frames_tx          =0
bcast_frames_tx          =2803
sml_frame_rcvd           =0

```

```

Software MAC address filter(hash:length/addr/mask/hits):
0x00: 0 ffff.ffff.ffff 0000.0000.0000 131803

```

2.6 Troubleshooting CPU Switch Module Memory

To troubleshoot the CPU switch module memory, use the following commands:

Command	Purpose
<code>show memory</code>	Shows statistics about the Cisco ONS 15530 memory, including free pool statistics.
<code>show buffers</code>	Displays statistics for the buffer pools on the Cisco ONS 15530.

Troubleshooting Cisco ONS 15530 CPU switch module memory is the same as troubleshooting any Cisco route processor. Refer to the “Troubleshooting Hardware and Booting Problems” chapter of the *Cisco IOS Internetwork Troubleshooting Handbook* for more information.

If the Cisco ONS 15530 fails, it is sometimes useful to get a full copy of the memory image, called a *core dump*, to identify the cause of the failure. Core dumps are generally only useful to your technical support representative. For troubleshooting information relating to system management and information about creating core dumps, refer to the *Cisco IOS Configuration Fundamentals Command Reference*.

2.7 Verifying Hardware and Software Versions

A common problem is an incompatibility between a hardware module and the Cisco IOS software version needed to perform a particular function. This section describes troubleshooting that problem.

Display the hardware and software versions to ensure that they are the most recent. Very old hardware and software versions (two or three versions back) can have caveats that have been fixed in more recent versions. Use the following EXEC commands to display version information:

Command	Purpose
<code>show version</code>	Displays the software version information.

Command	Purpose
show hardware [detail]	Displays detailed hardware information including revision level and version.
show functional-image slot slot	Displays functional image information.

To verify hardware and software versions, use the following steps:

Step 1 Issue the **show version** command to display the system software version on the active CPU switch module.

```
Switch# show version
```

```
Cisco Internetwork Operating System Software
→ IOS (tm) ONS-15530 Software (ONS15530-I-M), Version 12.2(20030711:0
04939) [sar-f-rep 108]
Copyright (c) 1986-2003 by cisco Systems, Inc.
Compiled Mon 14-Jul-03 14:44 by sar
Image text-base: 0x60010BDC, data-base: 0x60A30000

→ ROM: System Bootstrap, Version 12.1(10r)EV, RELEASE SOFTWARE (fc1)

top uptime is 8 hours, 2 minutes
System returned to ROM by RPR Switchover at 20:01:26 UTC Fri Jun 23 2000
System image file is "bootflash:ons15530-i-mz.sar-f-rep"

cisco ONS15530 (RM7000) processor with 49152K/16384K bytes of memory.
R7000 CPU at 234Mhz, Implementation 39, Rev 2.1, 256KB L2, 2048KB L3 Cache

Last reset from s/w nmi
2 FastEthernet/IEEE 802.3 interface(s)
509K bytes of non-volatile configuration memory.

16384K bytes of Flash internal SIMM (Sector size 256K).
Standby CPU is up
Standby CPU has 49152K/16384K bytes of memory.
error - a Software forced crash, PC 0x602C1830
ONS-15530 Software (ONS15530-I-M), Experimental Version 12.2(20030711:004939) [s
ar-f-rep 108]
Compiled Mon 14-Jul-03 14:44 by sar
Image text-base: 0x60010BDC, data-base: 0x60A30000

Stack trace from system failure:
FP: 0x625BF990, RA: 0x602C1830
FP: 0x625BF9C0, RA: 0x6008DB90
FP: 0x625BF9F8, RA: 0x625BFA88
FP: 0x625BF9F8, RA: 0x602BF5D0
FP: 0x625BFA18, RA: 0x60623578
FP: 0x625BFA60, RA: 0x6062376C
FP: 0x625BFCE8, RA: 0x60620998
FP: 0x625BFD58, RA: 0x6060B7D4

Configuration register is 0x2
```

Step 2 Verify the ROM field. It indicates the release of Cisco IOS software loaded and running on the active CPU switch module.

Step 3 Issue the **show hardware** command to display the hardware revision levels for the CPU switch modules.


```

Switch# show hardware
-----
ONS 15530 Chassis, ETSI Version named Switch, Date: 04:04:48 UTC Sat Jun 24 2000
-----

Back-Plane Information
-----
Orderable Product No.  MAC-Address          MAC-Size  Serial No.   Mfg. Date  H/W Ver
-----
15530-CHAS-E=          00-09-7c-1a-cb-50 16         TBC06101005 2002/06/24 3.1

-----
Slot Orderable Product No.   Part No.   Rev  Serial No.   Mfg. Date  H/W Ver.
-----
0/0  PROTO-HAMPTONS-MUX/DEMUX  73-7399-01 2   CAB0603MBAX 01/30/2002 1.0
0/1  PROTO-HAMPTONS-MUX/DEMUX  73-7399-01 2   CAB0603MB91 01/30/2002 1.0
→ 5/* 15530-CPU=              73-6572-06 C0   CNH0651006X 01/21/2003 6.1
→ 6/* 15530-CPU=              73-6572-06 C0   CNH0651006L 01/14/2003 6.1

Power Supply:
Slot Part No.           Rev  Serial No.  RMA No.    Hw Vrs  Power Consumption
-----
Power Supply 0 Not present
Unable to read idprom for 1
Power Supply 1 :
           type       : 600W AC
           status      : OK

```

Step 4 Verify that the hardware versions listed in the H/W Ver column for the CPU switch modules in slots 5 and 6 are the same. If the hardware versions are not the same, continue with the “2.8 Verifying Hardware and Software Compatibility” section on page 2-13.

Step 5 Issue the **show hardware detail** command to display detailed information about the CPU switch module hardware, including the functional image versions.

```

Switch# show hardware detail
-----
ONS 15530 Chassis, ETSI Version named Switch, Date: 04:05:37 UTC Sat Jun 24 2000
-----

Back-Plane Information
-----
Slot Number           : N/A
Controller Type       : 0x1106
On-Board Description  : ONS 15530 Chassis, ETSI Version
Orderable Product Number: 15530-CHAS-E=
Board Part Number     : 73-6573-03
Board Revision        : 02
Serial Number         : TBC06101005
Manufacturing Date    : 2002/06/24
Hardware Version      : 3.1
RMA Number            : 0
RMA Failure Code      : 0
MAC Address           : 00-09-7c-1a-cb-50
MAC Address Block Size : 16

-----
Slot Number           : 0/0
Controller Type       : 0x1108
On-Board Description  : Prototype-Hamptons-MUX/DEMUX
Orderable Product Number: PROTO-HAMPTONS-MUX/DEMUX
Board Part Number     : 73-7399-01

```

2.7 Verifying Hardware and Software Versions

```

Board Revision      : 2
Serial Number       : CAB0603MBAX
Manufacturing Date  : 01/30/2002
Hardware Version    : 1.0
RMA Number          : 0x00
RMA Failure Code    : 0x00
-----
Slot Number         : 0/1
Controller Type     : 0x1108
On-Board Description : Prototype-Hamptons-MUX/DEMUX
Orderable Product Number: PROTO-HAMPTONS-MUX/DEMUX
Board Part Number   : 73-7399-01
Board Revision      : 2
Serial Number       : CAB0603MB91
Manufacturing Date  : 01/30/2002
Hardware Version    : 1.0
RMA Number          : 0x00
RMA Failure Code    : 0x00
-----
Slot Number         : 5/*
Controller Type     : 0x1100
On-Board Description : ONS 15530 CPU and Switch Board
Orderable Product Number: 15530-CPU=
Board Part Number   : 73-6572-06
Board Revision      : C0
Serial Number       : CNH0651006X
Manufacturing Date  : 01/21/2003
→ Hardware Version   : 6.1
RMA Number          :
RMA Failure Code    :
→ Functional Image Version: 1.43
Function-ID         : 0
-----
Slot Number         : 6/*
Controller Type     : 0x1100
On-Board Description : ONS 15530 CPU and Switch Board
Orderable Product Number: 15530-CPU=
Board Part Number   : 73-6572-06
Board Revision      : C0
Serial Number       : CNH0651006L
Manufacturing Date  : 01/14/2003
→ Hardware Version   : 6.1
RMA Number          :
RMA Failure Code    :
→ Functional Image Version: 1.43
Function-ID         : 0

Power Supply:
Slot Part No.      Rev Serial No.  RMA No.    Hw Vrs  Power Consumption
-----
Power Supply 0 Not present
Unable to read idprom for 1
Power Supply 1 :
                  type       : 600W AC
                  status      : OK

```

Step 6 Verify that the Hardware Version and Functional Image Version fields for the CPU switch modules in slots 5 and 6 are the same. If they are not the same, continue with the following process to confirm that they are compatible.

Step 7 Use the **show functional-image** command to display detailed information about the functional images for the route processors, switch processors, and Fast Ethernet interface for the Cisco ONS 15530. The following example shows how to display the functional image for the route processor in slot 4:

```
Switch# show functional-image slot X
```

- Step 8** Verify the FunctionalVersion and #HardwareRequired fields to determine the FPGA version and the hardware version required for the FPGA. Compare this with the hardware version using the **show hardware** command output. If the FPGA version does not support the hardware version, download a new FPGA image, upgrade the hardware, or both.

2.8 Verifying Hardware and Software Compatibility

You can verify your hardware and software version compatibility by using the following EXEC command to display CPU switch module compatibility information:

Command	Purpose
show redundancy capability	Displays the software version compatibility information.
show functional-image slot <i>slot</i>	Displays functional image information.

To verify hardware and software compatibility of the CPU switch modules and modules, use the following steps:

- Step 1** Issue the **show redundancy capability** command to display the system software version compatibility with the various modules installed.

```
Switch# show redundancy capability
```

```
CPU capability support
```

```

Active CPU   Sby CPU   Sby Compat   CPU capability description
-----
→ 48 MB      48 MB    OK           CPU DRAM size
→ 16 MB      16 MB    OK           CPU PMEM size
→ 512 KB     512 KB   OK           CPU NVRAM size
   16 MB     16 MB    OK           CPU Bootflash size
→ 6.1        6.1      OK           CPU hardware major.minor version
→ 1.43       1.43     OK           CPU functional major.minor version

```

```
→ Linecard driver major.minor versions, (counts: Active=13, Standby=13)
```

```

Active CPU   Sby CPU   Sby Compat   Drv/Ch/F ID   Driver description
-----
   1.3        1.3      OK           0x1100/0/0    CPU with Switch Fabric
   2.3        2.3      OK           0x1101/0/0    10 Port ESCON line card
   2.1        2.1      OK           0x110A/0/0    8 Port GE-FC line card
   3.1        3.1      OK           0x1105/0/0    2.5G Transparent line card
   1.9        1.9      OK           0x1105/1/0    2.5G Transparent line card
   3.1        3.1      OK           0x1109/0/0    2.5G Transparent line card
   1.9        1.9      OK           0x1109/1/0    2.5G Transparent line card
Active CPU   Sby CPU   Sby Compat   Drv/Ch/F ID   Driver description
-----
   1.3        1.3      OK           0x1103/0/0    OSC line card
   0.1        0.1      OK           0x1107/1/0    OSC daughter card
   2.1        2.1      OK           0x1102/0/0    10G trunk card
   1.0        1.0      OK           0x110B/0/0    2.5G trunk card

```

2.8 Verifying Hardware and Software Compatibility

```

2.1      2.1      OK          0x1110/0/0  PSM wdm splitter
1.1      1.1      OK          0x1100/0/1  ONS15530 Rommon

```

- Software sync client versions, listed as version range X-Y.
 X indicates the oldest peer version it can communicate with.
 Y indicates the current sync client version.
 Sync client counts: Active=6, Standby=6

```

Active CPU  Sby CPU  Sby Compat  Cl ID  Redundancy Client description
-----
ver 1-2    ver 1-2    OK          17    CPU Redundancy
ver 1-1    ver 1-1    OK          19    Interface Sync
ver 1-1    ver 1-1    OK          36    MetOpt Password Sync
ver 1-2    ver 1-2    OK          18    Online Diagnostics
ver 1-2    ver 1-2    OK          6     OIR Client
ver 1-1    ver 1-1    OK          27    metopt cm db sync

```

- Backplane IDPROM comparison

```

Backplane IDPROM field  Match  Local CPU  Peer CPU
-----
idversion               YES    1          1
magic                  YES    153       153
card_type               YES    4358      4358
order_part_num_str     YES    15530-CHAS-E= 15530-CHAS-E=
description_str        YES    ONS 15530 Chassis, ETSI Version
                        ONS 15530 Chassis, ETSI
Version
board_part_num_str     YES    73-6573-03 73-6573-03
board_revision_str     YES    02         02
serial_number_str      YES    TBC06101005 TBC06101005
date_of_manufacture_str YES    2002/06/24 2002/06/24
deviation_numbers_str  YES    0          0
manufacturing_use      YES    0          0
rma_number_str         YES    0          0
rma_failure_code_str   YES    0          0
oem_str                YES    Cisco_Systems Cisco_Systems
clei_str               YES
snmp_oid_substr       YES    3.326     3.326
schematic_num_str      YES    92-4568-03 92-4568-03
hardware_major_version YES    3          3
Backplane IDPROM field  Match  Local CPU  Peer CPU
-----
hardware_minor_version YES    1          1
engineering_use_str    YES
crcl6                  OK    26352     9285
user_track_string      YES
diagst                 YES    ^A        ^A
board_specific_revision YES    1          1
board_specific_magic_number YES    153       153
board_specific_length  YES    56        56
mac_address_block_size YES    16        16
mac_address_base_str   YES    00097c1acb50 00097c1acb50
cpu_number             OK    0          1
optical_backplane_type YES    255       255

```

- Step 2** Check the CPU memory sizes and versions in the CPU Capability Description column. The numbers in the Active CPU and Sby CPU (Standby CPU) columns should match. If not, check the Sby Compat (Standby Compatibility) column. If this column indicates the values are OK, then these values will function as compatible redundant CPU switch modules. If not, swap the CPU switch modules with versions that are compatible.

- Step 3** Check the CPU hardware major.minor versions and CPU functional major.minor versions in the CPU Capability Description column. The numbers in the Active CPU and Sby CPU (Standby CPU) columns should match. If not, check the Sby Compat (Standby Compatibility) columns. If this column indicates the values are OK, then these values will function as compatible redundant CPU switch modules. If not, swap the CPU switch modules with versions that are compatible.
- Step 4** Check the information in the Linecard driver section of the display. This section shows the compatibility of the software versions installed on the active and standby CPU switch modules with the various modules installed in the system.
- Step 5** Check the Sby Compat (Standby Compatibility) and the Driver description columns. An OK in the Sby Compat column indicates the software version installed on the CPU switch modules supports the drivers on the modules listed.
- Step 6** Check the Software sync client version section of the display. The Active CPU, Sby CPU and Redundancy Client description columns indicate the software versions the two CPU switch modules can use to synchronize their configurations. The version range in the display, shown as X-Y, indicates oldest-current peer client versions. For example, if the version lists 1-2, that indicates version 1 is the oldest version that the current version 2 could synchronize with its configuration.
- Step 7** Check the Backplane IDPROM comparison section of the display. Check the Match column. This indicates which elements match, are acceptable, or fail. Some elements do not match but the range is acceptable. For example, the crc16 elements fields never match because the information in the IDPROMs of the two CPU switch modules are different so the checksums never match. But they do appear as OK or compatible.

If any of the drivers are not supported or appear as OK, try updating the images installed on the CPU switch modules. Use the information in the “1.10 Checking Release Notes for Workarounds” section on page 1-16 to upgrade to a more recent version. That should solve a CPU switch module image compatibility problem.

2.9 Troubleshooting Redundant CPU Switch Modules

The Cisco ONS 15530 supports fault tolerance by allowing a standby CPU switch module to take over if the active CPU switch module fails. This standby, or redundant, CPU switch module runs in hot-standby mode. In hot-standby mode, the standby CPU switch module is partially booted with the Cisco IOS software; however, no configuration is loaded.

At the time of a switchover, the standby CPU switch module takes over as the active CPU switch module and loads the configuration as follows:

- If the running configurations on the active and standby CPU switch module match, the new active CPU switch module uses the running configuration file.
- If the running configurations on the active and standby CPU switch modules do not match, the new active CPU switch module uses the last saved configuration file in its NVRAM (not the NVRAM of the former active CPU switch module).

The former active CPU switch module then becomes the standby CPU switch module.



Note

If the standby CPU switch module is unavailable, a major alarm is reported. Issue the **show facility-alarm status** command to display the redundancy alarm status.

For redundant CPU switch modules to function correctly, your Cisco ONS 15530 CPU switch modules must meet the following requirements:

- Both CPU switch modules must have compatible hardware configurations.
- ROMMON version 12.1(10r)EV.
- Both CPU switch modules must have compatible releases of Cisco IOS software.

A common error you may encounter is the incompatibility of hardware modules and the Cisco IOS software version needed to perform a particular function.

2.9.1 Verifying Hardware and Software Versions of Redundant CPU Switch Modules

To troubleshoot the CPU switch module hardware and software versions for redundancy, use the following commands:

Command	Purpose
show version	Displays the system software version.
show hardware detail	Displays the hardware and software configurations of the active and standby CPU switch modules.
show version	Displays the CPU switch module software version information.
show redundancy	Displays the hardware and software configurations of the active and standby CPU switch module cards.
show redundancy capability	Displays capabilities for the active and standby processors.

To confirm that your system CPU switch modules meet the redundancy requirements, complete the following steps:

- Step 1** Use the **show version** command to confirm the system hardware and software status of the active CPU switch module.

```
Switch# show version
```

```
Cisco Internetwork Operating System Software
IOS (tm) ONS-15540 Software (manopt-M0-M), 12.1(X:X)
Copyright (c) 1986-2001 by cisco Systems, Inc.
Compiled Fri 23-Feb-01 15:23 by ffrazier
Image text-base:0x60010950, data-base:0x604E8000
```

```
→ ROM:System Bootstrap, Version 12.1(X:X)
BOOTFLASH:ONS-15540 Software (manopt-M0-M), 12.1(X:X)
```

```
Switch uptime is 30 minutes
System returned to ROM by power-on
System image file is "tftp://test/eng/manopt-m0-mz.010223.6"
```

```
cisco (QUEENS-CPU) processor with 98304K/32768K bytes of memory.
```

```
R7000 CPU at 234Mhz, Implementation 39, Rev 2.1, 256KB L2, 2048KB L3 Cache
```

```
Last reset from power-on
2 Ethernet/IEEE 802.3 interface(s)
509K bytes of non-volatile configuration memory.
```

```
20480K bytes of Flash PCMCIA card at slot 0 (Sector size 128K).
16384K bytes of Flash internal SIMM (Sector size 64K).
Configuration register is 0x102
```

Step 2 Verify the ROM field. It indicates the release of Cisco IOS software loaded and running on the active CPU switch module.

Step 3 Use the **show hardware detail** command to compare the hardware versions of the active and standby CPU switch modules.

```
Switch# show hardware detail
-----
named Switch, Date: 04:36:29 UTC Fri Apr 20 2001
-----
.
{Information Deleted}
.
-----
Slot Number           : 6
Controller Type       : Queens CPU
On-Board Description  : Queens_CPU_PHASE_0
Orderable Product Number: N/A
Board Part Number     : 73-5621-02
Board Revision        : 03
Serial Number         : CAB0505GZHD
Manufacturing Date    : 02/16/2001
→ Hardware Version    : 2.1
RMA Number            : 0x00
RMA Failure Code      : 0x00
Functional Image Version: 1.8
-----
Slot Number           : 7
Controller Type       : Queens CPU
On-Board Description  : Queens_CPU_PHASE_0
Orderable Product Number: N/A
Board Part Number     : 73-5621-02
Board Revision        : 03
Serial Number         : CAB0505GZHV
Manufacturing Date    : 02/16/2001
→ Hardware Version    : 2.1
RMA Number            : 0x00
RMA Failure Code      : 0x00
Functional Image Version: 1.11
-----
Back-Plane EEPROM
-----
Slot Number           : N/A
Controller Type       : N/A
On-Board Description  :
Orderable Product Number:
Board Part Number     :
Board Revision        :
Serial Number         :
Manufacturing Date    : 01/01/2000
Hardware Version      : 0.0
RMA Number            : 0x00
```

2.9.1 Verifying Hardware and Software Versions of Redundant CPU Switch Modules

```

RMA Failure Code          : 0x00
Optical Back-Plane Type  : Unknown Optical Backplane
MAC Address               : 00-ab-00-00-00-
MAC Address Block Size   : 1

```

```

-----
Power-Supply Module
-----

```

```

Primary Power-Supply is : Not working
Backup Power-Supply is  : Not working

```

- Step 4** In the slots labeled 6 and 7, compare the Image version fields. These numbers must all match or be compatible, otherwise redundancy will not function correctly on your Cisco ONS 15530. For additional information, see the “2.7 Verifying Hardware and Software Versions” section on page 2-9.

To troubleshoot the hardware and software versions on redundant CPU switch module, use the following steps:

- Step 1** Issue the **show version** command to display the system software version on the active CPU switch module as described in the “2.7 Verifying Hardware and Software Versions” section on page 2-9.

- Step 2** Issue the **show redundancy summary** command to check the configuration and status of the active and standby CPU switch module.

```
Switch# show redundancy summary
```

```
Redundant system information
```

```
-----
Available Uptime:          12 hours, 50 minutes
sysUpTime (switchover clears): 7 hours, 52 minutes
Switchover Count:         5

```

```

Inter-CPU Communication State: UP
Last Restart Reason:         Switch over
Reported Switchover Reason:  Active unit failed (error - a Software forced cra
sh, PC 0x602C1830)
Software state at switchover: STANDBY HOT

```

- Last Running Config sync: 7 hours, 52 minutes
- Running Config sync status: In Sync
- Last Startup Config sync: 7 hours, 52 minutes
- Startup Config sync status: In Sync

```
This CPU is the Active CPU.
```

- Slot: 5
- Time since CPU Initialized: 8 hours, 7 minutes
- Image Version: ONS-15530 Software (ONS15530-I-M), Experimental V
- ersion 12.2(20030711:004939) [sar-f-rep 108]
- Image File: bootflash:ons15530-i-mz.sar-f-rep
- Software Redundancy State: ACTIVE
- Hardware State: ACTIVE
- Hardware Severity: 0

```
Peer CPU is the Standby CPU.
```

- Slot: 6
- Time since CPU Initialized: 7 hours, 52 minutes
- Image Version: ONS-15530 Software (ONS15530-I-M), Version
- 12.2(20030711:004939) [sar-f-rep 108]
- Image File (on sby-CPU): bootflash:ons15530-i-mz.sar-f-rep
- Software Redundancy State: STANDBY HOT
- Hardware State: STANDBY


```
Hardware Severity:          0
Privilege Mode:           Enabled
```

- Step 3** Verify the Last Running Config sync and Last Startup Config sync fields. They indicate the last time the running configuration and startup configuration were synchronized between the CPU switch modules.
- Step 4** Verify the active, standby, and Slot fields. They indicate in which slot the active CPU switch module is configured.

2.9.2 Verifying Redundant CPU Switch Module Functions

To troubleshoot the CPU switch module function capabilities and redundancy, use the following commands:

Command	Purpose
show redundancy capability	Displays capabilities for the active and standby CPU switch modules.
show redundancy clients	Displays internal redundancy software client information, which can be used to debug redundancy software.
show redundancy counters	Displays internal redundancy software counter information, which can be used to debug redundancy software.
show redundancy history	Displays the internal redundancy software history log, which can be useful for debugging redundancy software.
show redundancy running-config-file	Displays the running-config-file on the standby CPU switch module.
show redundancy states	Displays internal redundancy software state information.

Follow these steps to troubleshoot CPU switch module and redundancy capabilities on the system:

- Step 1** Issue the **show redundancy capability** command to display capabilities of the active or standby CPU switch modules described in the “2.7 Verifying Hardware and Software Versions” section on page 2-9.
- Step 2** Check the CPU memory sizes and versions in the column, CPU capability description. The numbers in the columns Active CPU and Sby CPU (Standby CPU) should match. If not, check the column, Sby Compat (Standby Compatibility). If this column indicates the values are OK then these values will function as compatible redundant CPU switch modules. If not, swap the CPU switch modules with versions that are compatible.
- Step 3** Check the CPU hardware and functional major.minor versions in the column, CPU capability description. The numbers in the columns Active CPU and Sby CPU (Standby CPU) should match. If not, check the column, Sby Compat (Standby Compatibility). If this column indicates the values are OK then these values will function as compatible redundant CPU switch modules. If not, swap the CPU switch modules with versions that are compatible.

- Step 4** Check the information in the column Driver description. This column lists the hardware drivers on the system components that are supported by the CPU switch module version for both the Active and Sby (Standby) CPU switch modules. OK indicates both versions of CPU switch modules support these drivers.
- Step 5** Check the Software sync client version section of the display. The Active and Sby CPU columns Redundancy Client description columns indicate the software versions the two CPU switch modules can use to synchronize their configurations. The version range in the display, shown as X-Y, indicates oldest-current peer client versions. For example, if the version lists 1-2, that indicates version 1 is the oldest version that the current version 2 could synchronize with its configuration.

- Step 1** Check the IDPROM comparison section of the display. Check the Match column. This indicates which elements match, are acceptable, or fail. Some elements do not match but the range is acceptable. For example, the crc16 elements fields never match because the information in the IDPROMs of the two CPU switch modules are different so the checksums never match. But they do appear as OK or compatible.

- Step 2** Issue the **show redundancy clients** command to display a list of internal redundancy clients.

```
Switch# show redundancy clients

clientID = 0      clientSeq = 0      RF_INTERNAL_MSG
clientID = 6      clientSeq = 180    OIR Client
clientID = 7      clientSeq = 190    APS
clientID = 17     clientSeq = 230    CPU Redundancy
clientID = 18     clientSeq = 280    Online Diagnostics
clientID = 19     clientSeq = 300    Interface Sync
clientID = 27     clientSeq = 330    metopt cm db sync
clientID = 35     clientSeq = 360    History RF Client
clientID = 36     clientSeq = 370    MetOpt Password Sync
clientID = 65000  clientSeq = 65000  RF_LAST_CLIENT
```

- Step 3** Issue the **show redundancy counters** command to display internal redundancy software counters.

```
Switch# show redundancy counters

Redundancy Facility OMs
  comm link up = 2
  comm link down down = 1

  invalid client tx = 1
  null tx by client = 0
  tx failures = 1
  tx msg length invalid = 0

  client not rxing msgs = 0
  rx peer msg routing errors = 0
  null peer msg rx = 0
  errored peer msg rx = 0

  buffers tx = 2668
  tx buffers unavailable = 0
  buffers rx = 10858
  buffer release errors = 0

  duplicate client registers = 0
  failed to register client = 0
  Invalid client syncs = 0
```

- Step 4** Issue the **show redundancy history** command to display internal redundancy software history.

```
Switch# show redundancy history
```

```

4w5d client added: RF_INTERNAL_MSG(0) seq=0
4w5d client added: RF_LAST_CLIENT(65000) seq=65000
00:00:00 client added: History RF Client(35) seq=360
00:00:01 client added: CPU Redundancy(17) seq=230
00:00:02 client added: Interface Sync(19) seq=300
00:00:02 client added: MetOpt Password Sync(36) seq=370
00:00:02 *my state = INITIALIZATION(2) *peer state = DISABLED(1)
00:00:02 RF_PROG_INITIALIZATION(100) RF_INTERNAL_MSG(0) op=0 rc=11
00:00:02 RF_PROG_INITIALIZATION(100) CPU Redundancy(17) op=0 rc=11
00:00:02 RF_PROG_INITIALIZATION(100) Interface Sync(19) op=0 rc=11
00:00:02 RF_PROG_INITIALIZATION(100) History RF Client(35) op=0 rc=11
00:00:02 RF_PROG_INITIALIZATION(100) MetOpt Password Sync(36) op=0 rc=11
00:00:02 RF_PROG_INITIALIZATION(100) RF_LAST_CLIENT(65000) op=0 rc=11
00:00:02 *my state = NEGOTIATION(3) peer state = DISABLED(1)
00:00:02 RF_STATUS_PEER_PRESENCE(400) op=1
00:00:02 RF_STATUS_PEER_PRESENCE(400) CPU Redundancy(17) op=1
00:00:02 RF_STATUS_PEER_PRESENCE(400) Interface Sync(19) op=1
00:00:02 RF_STATUS_PEER_PRESENCE(400) MetOpt Password Sync(36) op=1
00:00:03 RF_STATUS_PEER_COMM(401) op=1
00:00:03 RF_STATUS_PEER_COMM(401) CPU Redundancy(17) op=1
00:00:03 RF_STATUS_PEER_COMM(401) Interface Sync(19) op=1
00:00:03 RF_STATUS_PEER_COMM(401) MetOpt Password Sync(36) op=1
00:15:12 RF_EVENT_PEER_PROG_DONE(506) RF_LAST_CLIENT(65000) op=105
00:15:16 *my state = ACTIVE(13) *peer state = STANDBY HOT(8)

```

Information deleted-----

Step 5 Issue the **show redundancy running-config-file** command to display running configuration on the standby CPU switch module.

```

sby-Switch# show redundancy running-config-file
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service internal
!
hostname top
!
boot system bootflash:ons15530-i-mz.sar-f-rep
boot bootldr bootflash:ons15530-i-mz.sar-f-rep
logging snmp-authfail
logging queue-limit 100
logging buffered 10000 debugging
enable password lab
!
diag online
no diag power-on
ip subnet-zero
ip ftp source-interface FastEthernet0
ip ftp username rhino
ip ftp password godzilla
no ip domain-lookup
!
!
!
!
!
Information deleted-----
end
^@^@

```

Step 6 Issue the **show redundancy states** command to display internal redundancy software state information.

```
Switch# show redundancy states
→ my state = 13 -ACTIVE
→ peer state = 8 -STANDBY HOT
    Mode = Duplex
    Unit ID = 5

    Split Mode = Disabled
    Manual Swact = Enabled
    Communications = Up

    client count = 10
    client_notification_TMR = 30000 milliseconds
    keep_alive TMR = 12000 milliseconds
    keep_alive count = 0
    keep_alive threshold = 17
    RF debug mask = 0x0
```

Refer to the *Cisco ONS 15530 Configuration Guide* and the *Cisco ONS 15530 Command Reference* for the following:

- Configuring CPU switch module redundancy
- Upgrading the software image on the redundant CPU switch module
- Downloading the system image on the CPU switch modules

2.10 Troubleshooting CPU Switch Module Problems

This section includes CPU switch module troubleshooting procedures.

2.10.1 Active CPU Switch Module Boot Failure

Symptom The active CPU switch module fails to boot.

Table 2-1 describes the potential causes of the symptom and the solutions.

Table 2-1 Active CPU Switch Module Boot Failure

Possible Problem	Solution
Auto boot not configured.	Manually boot the valid system image, then issue the config reg 0x2102 command to configure auto boot.
Invalid boot configuration.	Manually boot the valid system image and check the boot system configuration. Correct the configuration if necessary.

2.10.2 Standby CPU Switch Module Boot Failure

Symptom The standby CPU switch module fails to boot.

Table 2-2 describes the potential causes of the symptom and the solutions.

Table 2-2 Standby CPU Switch Module Boot Failure

Possible Problem	Solution
Auto boot not configured.	Manually boot the valid system image, then issue the config reg 0x2102 command to configure auto boot.
Invalid boot configuration.	Manually boot the valid system image and check the boot system configuration. Correct the configuration if necessary.
Peer (active) CPU switch module reset.	Issue the show redundancy history , show redundancy state , show redundancy events , show redundancy clients , and the show buffers commands and provide the outputs to Cisco technical support.

2.10.3 Unable to Access CPU Switch Module Console

Symptom The CPU switch module console cannot be accessed.

Table 2-3 describes the potential causes of the symptom and the solutions.

Table 2-3 Unable to Access Switch Module Console

Possible Problem	Solution
Console cable.	Verify that the console cable is connected properly, and replace if necessary.
Incorrect termserver setting.	Check the termserver configuration, and correct the settings if necessary.

2.10.4 Unable to Access Enable Mode on Active CPU Switch Module

Symptom The system does not allow access to the enable mode.

Table 2-4 describes the potential causes of the symptom and the solutions.

Table 2-4 Unable to Access Enable Mode

Possible Problem	Solution
Password incorrect.	Perform the password recovery procedure. See the “2.4 Recovering a Lost Password” section on page 2-4.

2.10.5 Unable to Access Enable Mode on Standby CPU Switch Module

Symptom The system does not allow access to the enable mode on the standby CPU switch module. Table 2-4 describes the potential causes of the symptom and the solutions.

Table 2-5 *Unable to Access Enable Mode*

Possible Problem	Solution
Password incorrect.	Perform the password recovery procedure. See the “2.4 Recovering a Lost Password” section on page 2-4.
Password synchronization.	Check the image on the active and standby CPU switch modules. Update to the latest image if necessary. If the images are the same, issue the show tech and the show log commands and provide the outputs to Cisco technical support.



Troubleshooting Transponder Line Card Problems

This chapter describes how to troubleshoot transponder line card problems. This chapter includes the following sections:

- 3.1 Overview, page 3-1
- 3.2 Initial Troubleshooting Checklist, page 3-2
- 3.3 Troubleshooting Transponder Line Card Problems, page 3-3
- 3.4 Troubleshooting Transponder Line Card Problems Using Loopbacks, page 3-7

3.1 Overview

The protocol-transparent and bit-rate transparent transponder line card converts a client signal into an ITU wavelength, or channel. The transponder line cards have tunable lasers and you can configure the line cards to work in two different wavelengths.

The Cisco ONS 15530 supports four types of client interface transponder line cards: SM (single mode) unprotected, SM splitter protected, MM (multimode) unprotected, and MM splitter protected. Both types of SM transponder line cards accept SM client signals on the 1310-nm wavelength through an SC connector and support client signal clock rates ranging from 16 Mbps to 2.5 Gbps. Both types of MM transponder line cards accept SM and MM client signals on the 1310-nm wavelength through an SC connector and support client signal clock rates ranging from 16 Mbps to 622 Mbps.

Figure 3-1 and Figure 3-2 show the architecture and the interfaces of the transponder line card.

Figure 3-1 Transponder Line Card Architecture

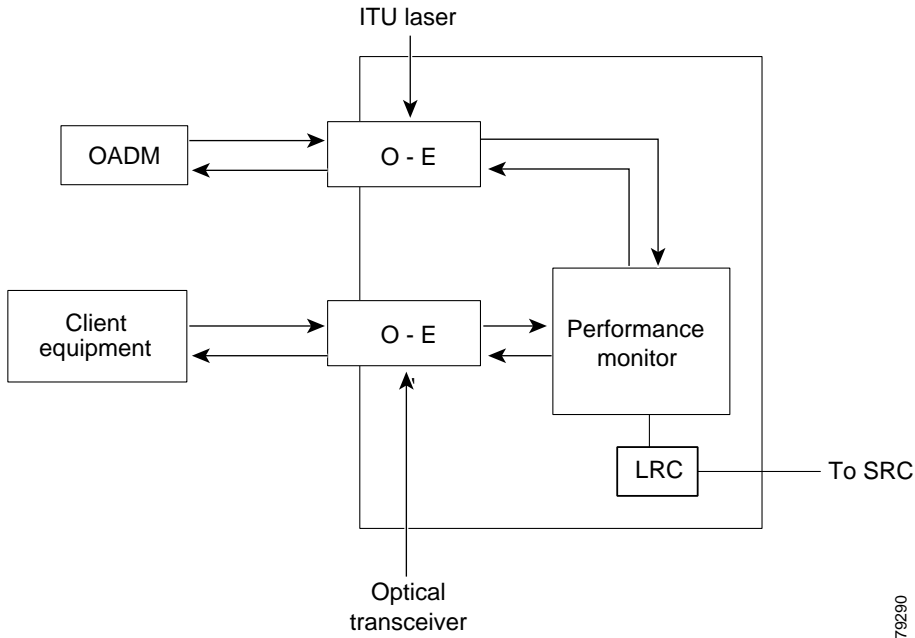
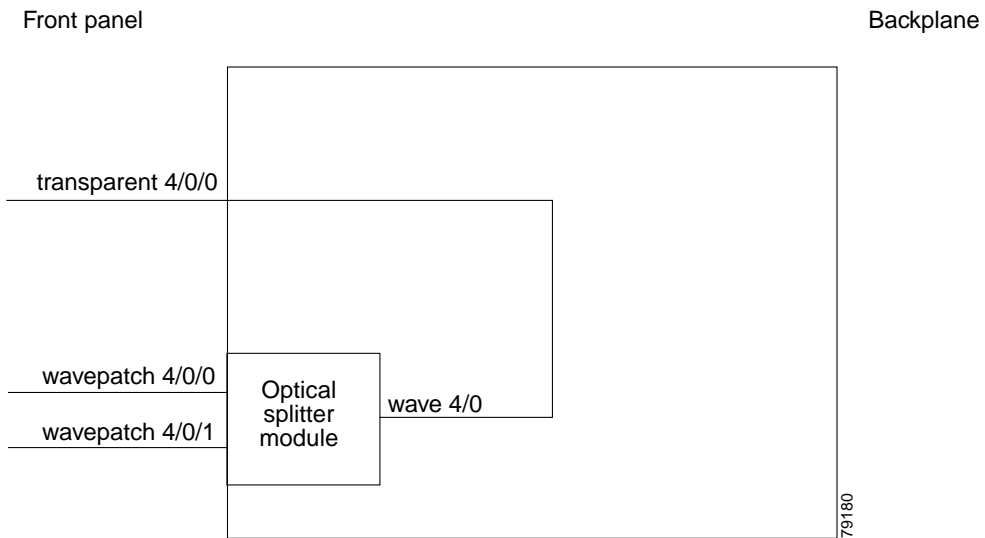


Figure 3-2 Transponder Line Card Interfaces



3.2 Initial Troubleshooting Checklist

Follow this initial checklist before proceeding with the troubleshooting procedures:

- Ensure encapsulation is set correctly.

- Enable monitoring if needed or supported.
- Ensure transparent, wave, and wavepatch interfaces are administratively up.
- Ensure proper cable (SM/MM) is connected according to the transponder type/traffic type.
- Ensure trunk receive power level is within valid range (-8 to -28 dBm).
- Ensure client receive power is within valid range (-5 dBm to -28/-32 dBm for SM/MM respectively).
- Check that Tx and Rx LEDs (client side and trunk side) are working as expected.
- Ensure optical threshold parameters do not force loss-of-light condition.
- Check that all error counters on the interfaces are clean.
- Ensure optical patches are properly configured according to the channel/wavelength.
- Check that laser frequency is properly programmed and **show patch** command output does not list a mismatch.
- Issue a **show facility-alarm status** command to display the alarms on the interfaces.
- Issue the **show hardware linecard** command to verify the transponder line card functional image.
- Ensure that all optical connectors are clean. Refer to the *Cisco ONS 15530 Cleaning Procedures for Fiber Optic Connections* document.

3.3 Troubleshooting Transponder Line Card Problems

This section contains troubleshooting procedures for transponder line card problems.

3.3.1 Transponder Line Card Not in show hardware Command Output

Symptom Transponder line card line is not listed in the **show hardware** command output.

Table 3-1 describes the potential causes of the symptom and the solutions.

Table 3-1 Transponder Line Card Not in show hardware Command Output

Possible Problem	Solution
Transponder line card not seated properly.	Reseat the transponder line card.
Incompatible software.	Verify the software supports the hardware being used.
Bad transponder line card.	Replace the transponder line card.

3.3.2 Wave Interface Is Down and Shows Loss of Light

Symptom The wave interface is down and shows Loss of Light.

Table 3-2 describes the potential causes of the symptom and the solutions.

Table 3-2 Wave Interface Is Down and Shows Loss of Light

Possible Problem	Solution
Incorrect cable connection or wrong cable being used.	Issue a show interfaces wave command to ensure the laser frequency is as desired and verify that no mismatch is present in the show patch command output.
Optical connectors are dirty.	Refer to the <i>Cisco ONS 15530 Cleaning Procedures for Fiber Optic Connections</i> document.
Incoming power level is low.	Use a power meter to check the power level from the OADM module to the wave interface of the transponder line card. Adjust attenuation as needed.

3.3.3 Transparent Interface Is Down and Shows Loss of Light

Symptom The transparent interface is down and shows Loss of Light.

Table 3-3 describes the potential causes of the symptom and the solutions.

Table 3-3 Transparent Interface Down and Shows Loss of Light

Possible Problem	Solution
Incorrect cable connection or wrong cable being used.	Issue a show interfaces transparent command to ensure the laser frequency is as desired and verify that no mismatch is present in the show patch command output. Verify that the correct cable type (SM/MM) is being used.
Optical connectors are dirty.	Refer to the <i>Cisco ONS 15530 Cleaning Procedures for Fiber Optic Connections</i> document.
Incoming power level is low.	Use a power meter to check the receive power level to the transparent interface of the transponder line card. Adjust attenuation as needed.

3.3.4 Active and Standby Wavepatch Interfaces Down Due to Loss of Light

Symptom The active and standby wavepatch interfaces are down due to Loss of Light.

Table 3-4 describes the potential causes of the symptom and the solutions.

Table 3-4 Wavepatch Interfaces Down Due to Loss of Light

Possible Problem	Solution
Incorrect cable connection or wrong cable being used.	Issue a show interfaces wave command to ensure the laser frequency is as desired and verify that no mismatch is present in the show patch command output.
Optical connectors are dirty.	Refer to the <i>Cisco ONS 15530 Cleaning Procedures for Fiber Optic Connections</i> document.
Incoming power level is low.	Use a power meter to check the power level from the client to the transponder line card.

3.3.5 Wave Interface Shows Loss of Lock

Symptom The wave interface shows Loss of Lock.

Table 3-5 describes the potential causes of the symptom and the solutions.

Table 3-5 Wave Interface Shows Loss of Lock

Possible Problem	Solution
Incorrect protocol.	Issue a show interfaces wave command to verify that the correct protocol is configured and monitoring is enabled if needed.
Remote client reporting errors.	Issue a show interfaces transparent command on the remote system to verify that the remote client interface is not reporting errors.
Optical connectors are dirty.	Refer to the <i>Cisco ONS 15530 Cleaning Procedures for Fiber Optic Connections</i> document.

3.3.6 Transparent Interface Shows Loss of Lock

Symptom The transparent interface shows Loss of Lock.

Table 3-6 describes the potential causes of the symptom and the solutions.

Table 3-6 Wave Interface Shows Loss of Lock

Possible Problem	Solution
Incorrect protocol.	Issue a show interfaces transparent command to verify that the correct protocol is configured and monitoring is enabled if needed.
Optical connectors are dirty.	Refer to the <i>Cisco ONS 15530 Cleaning Procedures for Fiber Optic Connections</i> document.

3.3.7 Interface Shows Loss of Sync

Symptom The wave or transparent interface shows Loss of Sync.

Table 3-7 describes the potential causes of the symptom and the solutions.

Table 3-7 Interface Shows Loss of Sync

Possible Problem	Solution
Incorrect protocol.	Issue a show interfaces command to verify that the correct protocol is configured and monitoring is enabled if needed.
Remote client reporting errors.	Issue a show interfaces transparent command on the remote system to verify that the remote client interface is not reporting errors.
Optical connectors are dirty.	Refer to the <i>Cisco ONS 15530 Cleaning Procedures for Fiber Optic Connections</i> document.

3.3.8 Interface Shows Loss of Frame

Symptom The wave or transparent interface shows Loss of Frame.

Table 3-8 describes the potential causes of the symptom and the solutions.

Table 3-8 *Interface Shows Loss of Frame*

Possible Problem	Solution
Incorrect protocol.	Issue a show interfaces command to verify that the correct protocol is configured and monitoring is enabled if needed.
Excessive attenuation.	Use a power meter to ensure that the receive power level is within specifications for that interface. Reduce the attenuation as needed.
Overload (high receive power).	Use a power meter to ensure that the receive power level is within specifications for that interface. Attenuate the receive path as needed.
Optical connectors are dirty.	Refer to the <i>Cisco ONS 15530 Cleaning Procedures for Fiber Optic Connections</i> document.

3.3.9 Active and Standby Wavepatch Interfaces Down Due to Low Alarm

Symptom The active and standby wavepatch interfaces are down due to low alarm.

Table 3-9 describes the potential causes of the symptom and the solutions.

Table 3-9 *Active and Standby Wavepatch Interfaces Down Due to Low Alarm*

Possible Problem	Solution
Excessive attenuation.	Use a power meter to ensure that the receive power level is within specifications for that interface.
Optical connectors are dirty.	Refer to the <i>Cisco ONS 15530 Cleaning Procedures for Fiber Optic Connections</i> document.
Optical threshold exceeded.	Issue a show interfaces wavepatch command to verify that the receive power is within the threshold range.

3.3.10 Unable to Configure Protocol Encapsulation or Clock Rate

Symptom The CLI (command-line interface) rejects the protocol encapsulation or clock rate for the transparent interface.

Table 3-10 describes the potential cause of the symptom and the solution.

Table 3-10 Unable to Configure Protocol Encapsulation or Clock Rate

Possible Problem	Solution
Incorrect transponder line card.	Verify that you have the correct type of transponder line card, either SM or MM. If not, replace it with the correct transponder line card.

3.4 Troubleshooting Transponder Line Card Problems Using Loopbacks

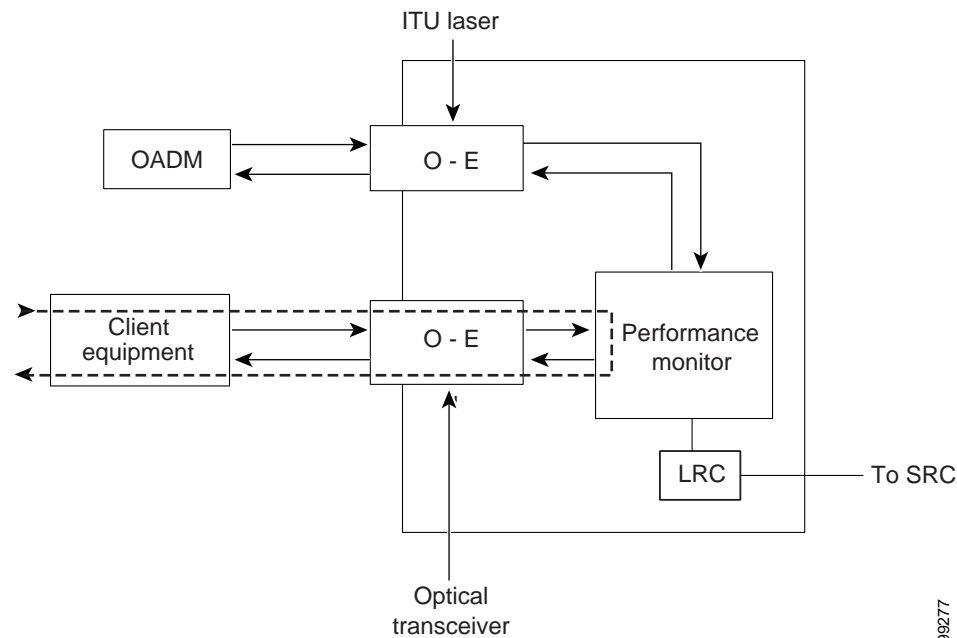
This section describes how to use software loopbacks to perform fault isolation on the client and trunk interfaces of the transponder line cards.

**Note**

Client and trunk loopbacks cannot be performed at the same time.

3.4.1 Client Signal Loopbacks

The client signal loopback verifies the continuity of the client signal path (see Figure 3-3).

Figure 3-3 Client Signal Loopback Example

Symptom Client signal loopback fails.

Table 3-11 describes the potential causes of the symptom and the solutions.

Table 3-11 Client Signal Loopback Fails

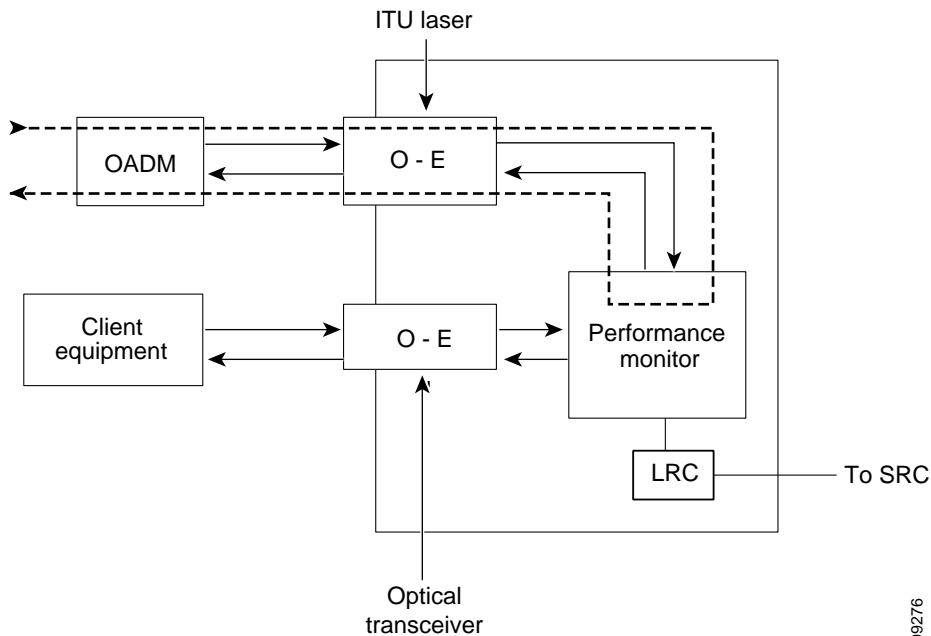
Possible Problem	Solution
Protocol not configured correctly.	Issue a show interfaces wave command to check the configured encapsulation. Issue a encapsulation command to correct the protocol encapsulation.
Client Tx/Rx power is insufficient.	Use a power meter to measure the power levels. Ensure that the Tx and Rx power levels are within specification.

Procedure: Create a Client Signal Loopback

-
- Step 1** Issue a **loopback** command on the transparent interface.
 - Step 2** Check that the traffic is reaching the client equipment.
 - Step 3** If the signal does not reach the client equipment, call Cisco technical support.
-

3.4.2 Trunk Loopbacks

The trunk loopback on a transponder line card verifies the configuration of the wave interface (see Figure 3-4).

Figure 3-4 Trunk Loopback Example

Symptom The trunk loopback fails.

Table 3-12 describes the potential causes of the symptom and the solutions.

Table 3-12 *Trunk Loopback Fails*

Possible Problem	Solution
Incorrect encapsulation.	Issue a show interface transparent command to check the configured encapsulation. Issue a encapsulation command to correct the protocol encapsulation.
Trunk power level is out of range.	Use a power meter to measure the power levels. Ensure that the Tx and Rx power levels are within specification.

Procedure: Create a Trunk Loopback

-
- Step 1** Issue a **loopback** command on the transparent interface.
 - Step 2** Check that the traffic is reaching the trunk.
 - Step 3** If the signal does not reach the trunk, call Cisco technical support.
-



Troubleshooting ESCON Aggregation Card Problems

This chapter describes how to troubleshoot ESCON aggregation card problems. This chapter includes the following sections:

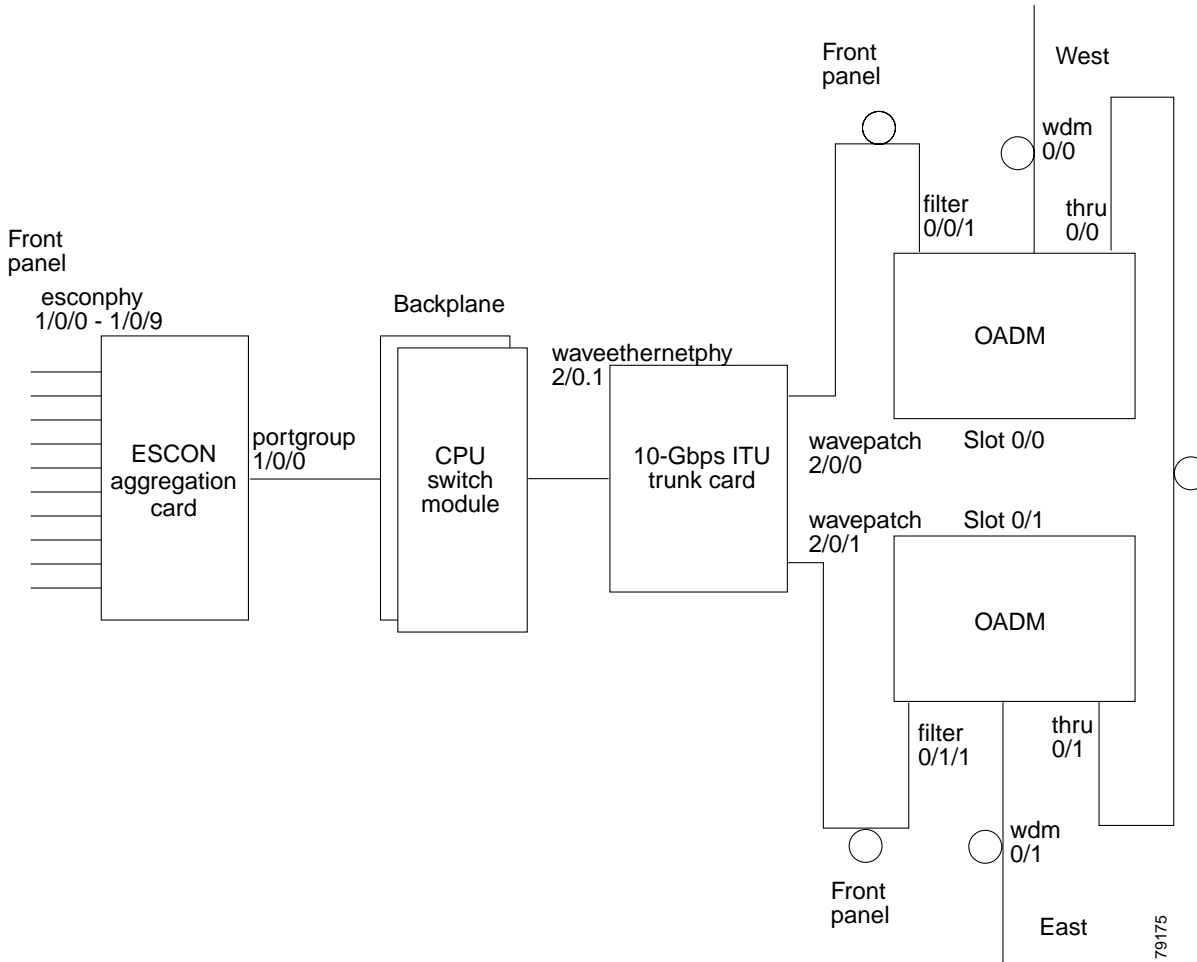
- 4.1 Overview, page 4-1
- 4.2 Initial Troubleshooting Checklist, page 4-2
- 4.3 Troubleshooting ESCON Aggregation Card Interface Problems, page 4-3
- 4.4 Troubleshooting ESCON Aggregation Card Problems Using Loopbacks, page 4-7

4.1 Overview

The ESCON aggregation card aggregates up to ten ESCON data streams into a single 2.5-Gbps signal, which is transmitted through the switch fabric to a 2.5-Gbps ITU trunk card, 10-Gbps ITU trunk card, 10-Gbps ITU tunable trunk card, or 10-Gbps uplink card. The ESCON aggregation card can be populated with up to ten SFP (small form-factor pluggable) optics.

Figure 4-1 shows an example path of an ESCON signal through the Cisco ONS 15530 and the associated interfaces.

Figure 4-1 Interface Model for ESCON Aggregation



4.2 Initial Troubleshooting Checklist

Follow this initial checklist before proceeding with the troubleshooting procedures:

- Check that the receive signal power level from the switch fabric is between -22 dBm and -6 dBm if the ESCON aggregation card is connected to a 10-Gbps ITU trunk card or a 10-Gbps ITU tunable trunk card, between -12.5 dBm and 0.5 dBm for a 10-Gbps uplink card, or between -28 dBm and -8 dBm for a 2.5-Gbps ITU trunk card.
- Check that the client receive signal power level is between -33 dBm and -14 dBm. If the receive signal power is not within this range, adjust the attenuation.
- Issue **show interfaces** commands to ensure that the `esconphy`, `waveethernetphy`, `wavepatch`, and `tengigethernetphy` interfaces are administratively up and that there are no errors on the interfaces.
- Issue a **show connect** command to verify the status of the cross connections between the ESCON aggregation card and the ITU trunk card or uplink card.
- Check that the LEDs on the card and SFP optics show the proper state.

- Issue a **show facility-alarm status** command to display the alarms on the interfaces.
- If ITU cards are present, check that the ITU cards are patched to the correct OADM ports. Issue a **show patch** command to verify that there are no frequency mismatches.
- Ensure that all optical connectors are clean. Refer to the *Cisco ONS 15530 Cleaning Procedures for Fiber Optic Connections* document.

4.3 Troubleshooting ESCON Aggregation Card Interface Problems

This section contains troubleshooting procedures for ESCON aggregation card interface problems.

4.3.1 Removing an SFP Optics Causes Alarms on Other Esconphy Interfaces

Symptom You removed one of the SFP optics on an ESCON aggregation card and alarm messages appear on the console for other interfaces on the same card.

Table 4-1 describes the potential cause of the symptom and the solution.

Table 4-1 *Removing an SFP Optics Causes Alarms on Other Esconphy Interfaces*

Possible Problem	Solution
The decrease in signal power caused forward laser control to shut down the interfaces.	Reinsert the SFP optics.

4.3.2 Shutting Down One Esconphy Interface Raises Alarms on Other Esconphy Interfaces

Symptom You shut down one esconphy interface and alarm messages appear on the console for other esconphy interfaces on the same ESCON aggregation card.

Table 4-2 describes the potential cause of the symptom and the solution.

Table 4-2 *Shutting Down One Esconphy Interface Raises Alarms on Other Esconphy Interfaces*

Possible Problem	Solution
The decrease in signal power caused forward laser control to raise the alarms.	Reenable the interface with a no shutdown command.

4.3.3 Reenabling an Esconphy Interface Clears Alarms on Other Esconphy Interfaces

Symptom You issued a **no shutdown** command on one esconphy interface and alarm messages appear on the console for other esconphy interfaces on the same ESCON aggregation card.

Table 4-3 describes the potential cause of the symptom and the solution.

Table 4-3 *Reenabling an Esconphy Interface Clears Alarms on Other Esconphy Interfaces*

Possible Problem	Solution
The increase in signal power caused forward laser control to clear the alarms.	None. This is normal behavior.

4.3.4 All Client Side Lasers Shut Down When Traffic to One Esconphy Interface Falls Below a Threshold

Symptom The client signal to one esconphy interface fell below an alarm threshold value which caused all client side lasers to shut down.

Table 4-4 describes the potential cause of the symptom and the solution.

Table 4-4 *All Client Side Lasers Shut Down When Traffic to One Esconphy Interface Falls Below a Threshold*

Possible Problem	Solution
The decrease in signal power caused forward laser control to shut down the interfaces.	<ol style="list-style-type: none"> 1. Check the signal from the client equipment and resolve the transmission problem. 2. Issue no shutdown commands on the shut down esconphy interfaces.

4.3.5 Client Side Laser Unexpectedly Shuts Down

Symptom A client side laser unexpectedly shuts down without affecting other client side lasers on the ESCON aggregation card.

Table 4-5 describes the potential causes of the symptom and the solutions.

Table 4-5 *Client Side Laser Unexpectedly Shuts Down*

Possible Problem	Solution
The interface at the remote end detects loss of light or is administratively shut down.	Correct the failure at the remote end.
The rate of traffic received from the remote end caused forward laser control to shut down the laser.	Correct the failure at the remote end.

4.3.6 Client Traffic Does Not Flow End-to-End

Symptom The client traffic does not reach the remote system.

Table 4-6 describes the potential causes of the symptom and the solutions.

Table 4-6 *Client Traffic Does Not Flow End-to-End*

Possible Problem	Solution
An interface in the path is administratively shut down.	Issue a show interfaces command for each interface on the signal path. If an interface is administratively shut down, use the no shutdown command on the interface.
The client receive signal power is not strong enough.	Check the Rx LED. If it is not on, make sure that the client receive signal power level is between -33 dBm and -14 dBm. Adjust the attenuation if the signal power is too low.
The cross connection is not properly configured.	Issue a show connect command to verify the configured cross connections. Correct any problems with the connect command.
The remote esconphy interface is not up.	<ol style="list-style-type: none"> 1. Check the Tx LED. 2. If the LED is not on, issue a show interfaces command on the remote system for the peer esconphy interface. 3. If the interface is not up, issue a no shutdown command on the remote esconphy interface.
The client laser is shut down by forward laser control.	Issue a show interfaces command for the esconphy interface to verify the status of the client side laser and the forward laser control configuration status. If forward laser control has shut down the laser, issue a show interfaces command on the remote system to verify the status of the peer esconphy interface and resolve any problems.

Table 4-6 Client Traffic Does Not Flow End-to-End (continued)

Possible Problem	Solution
Flow identifiers are not configured for all the esconphy interfaces and the ESCON traffic is mixing with GE traffic on a 10-Gbps ITU trunk card or a 10-Gbps ITU tunable trunk card.	<ol style="list-style-type: none"> 1. Issue a cdl flow identifier reserve command to reserve flow identifiers for all esconphy interfaces on the ESCON aggregation card, whether SFP optics is present for the interface or not. 2. Issue no shutdown commands on the esconphy interface present on card. <p>Note All existing flow identifiers take precedence over the reserve flow identifiers.</p>
Different CDL flow identifiers are configured on the esconphy interfaces.	Configure the same CDL flow identifiers on the corresponding esconphy interfaces on the two nodes.

4.3.7 Portgroup Interface Shows Continuous Errors

Symptom A portgroup interface reports continuous errors to the system console.

Table 4-7 describes the potential causes of the symptom and the solutions.

Table 4-7 Portgroup Interface Shows Continuous Errors

Possible Problem	Solution
A fault occurred in the switch fabric.	Issue a redundancy switch-activity command to switch over to the standby CPU switch module. If the switchover corrects the problem, replace the faulty CPU switch module.
A fault occurred in the ESCON aggregation card.	Perform signal loopbacks as described in the “4.4 Troubleshooting ESCON Aggregation Card Problems Using Loopbacks” section on page 4-7.

4.3.8 Esconphy Interface Not Created

Symptom A esconphy interface does not appear in the configuration and is not recognized by the system.

Table 4-8 describes the potential cause of the symptom and the solution.

Table 4-8 Esconphy interface not created

Possible Problem	Solution
Wrong SFP optics is installed.	Issue a show interfaces command for the esconphy interface and verify that the Optical Transceiver field shows a valid value. If not, replace the SFP optics with the correct part.

4.4 Troubleshooting ESCON Aggregation Card Problems Using Loopbacks

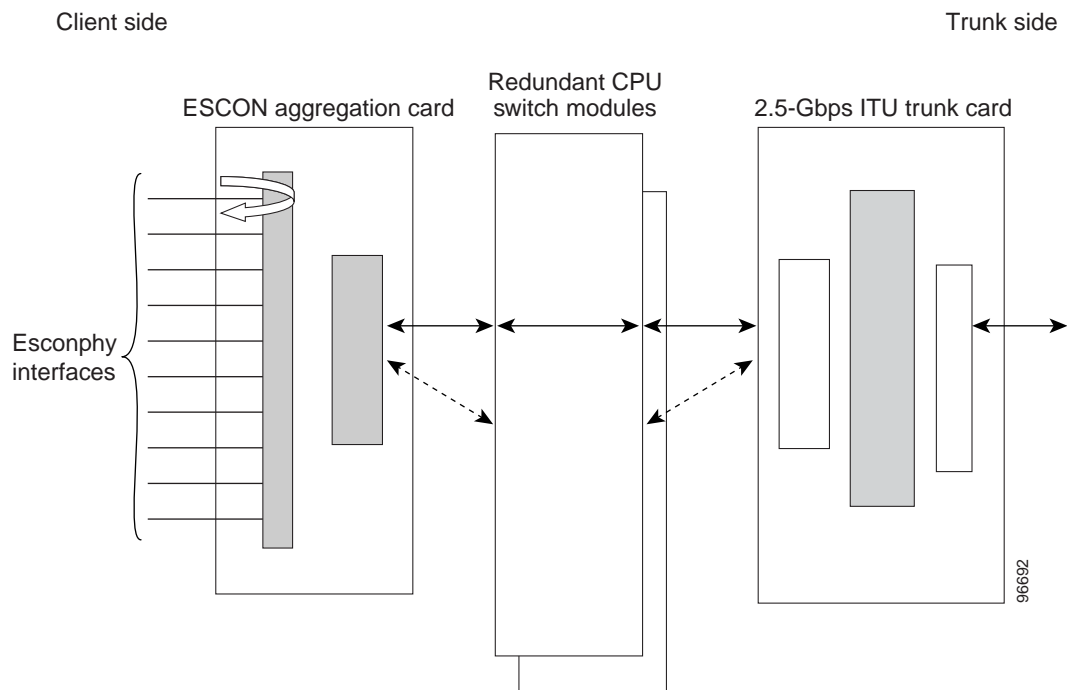
This section describes how to use software loopbacks to perform fault isolation for signals on ESCON aggregation cards.

To perform further loopback operations, see the “8.4 Troubleshooting 2.5-Gbps ITU Trunk Card Problems Using Loopbacks” section on page 8-5, “10.4 Troubleshooting 10-Gbps ITU Tunable Trunk Card Problems Using Loopbacks” section on page 10-6, and the “9.4 Troubleshooting 10-Gbps ITU Trunk Card Problems Using Loopbacks” section on page 9-5.

4.4.1 Client Signal Loopbacks

Client signal loopbacks on ESCON aggregation cards verify the functioning of the SFP optics (see Figure 4-2).

Figure 4-2 Client Signal Loopback Example



Procedure: Create a Client Signal Loopback

-
- Step 1** Issue a **loopback** command on the esconphy interface.
 - Step 2** Check that the traffic is reaching the client equipment.

Step 3 If the signal does not reach the client equipment, check the optical cables for breaks. If there are no breaks, replace the SFP optics.



Troubleshooting 4-Port 1-Gbps/2-Gbps FC Aggregation Card Problems

This chapter describes how to troubleshoot 4-port 1-Gbps/2-Gbps FC (Fibre Channel) aggregation card interface problems. This chapter includes the following sections:

- 5.1 Overview, page 5-1
- 5.2 Initial Troubleshooting Checklist, page 5-2
- 5.3 Troubleshooting 4-Port 1-Gbps/2-Gbps FC Aggregation Card Interface Problems, page 5-3
- 5.4 Troubleshooting Problems Using show controller Command Output, page 5-11
- 5.5 Troubleshooting 4-Port 1-Gbps/2-Gbps FC Aggregation Card Problems Using Loopbacks, page 5-16

5.1 Overview

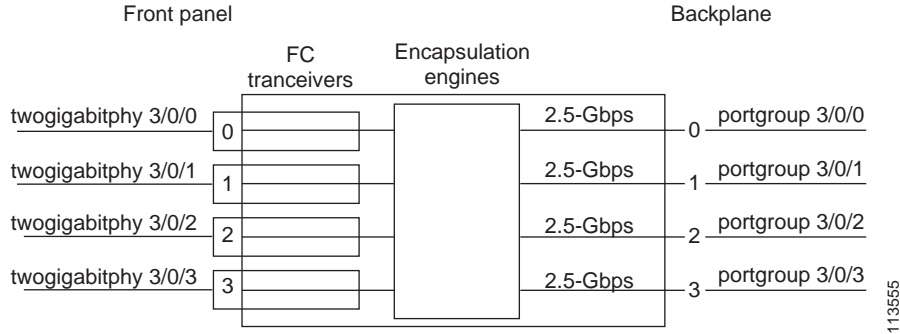
The 4-port 1-Gbps/2-Gbps FC aggregation card uses up to four SFP (small form-factor pluggable) optical transceivers to support client traffic. Each client interface can be configured using the CLI (command-line interface) for FC, FICON (fiber connection), or ISC (InterSystem Channel) traffic at a 1-Gbps or 2-Gbps rate.

The 4-port 1-Gbps/2-Gbps FC aggregation card connects four 2.5-Gbps electric signals, or portgroup interfaces, to the switch fabric. The client port data streams must be mapped to one of these portgroup interfaces, using the CLI. Only two 1-Gbps client interfaces or one 2-Gbps client interface can be mapped into a single portgroup interface.

The signal on the portgroup interfaces connects through the backplane and the switch fabric on the active CPU switch module to a 2.5-Gbps ITU trunk card, a 10-Gbps ITU trunk card, 10-Gbps ITU tunable trunk card, or a 10-Gbps uplink card, where the signal is converted to, and from, an ITU channel. The cross connections between the two cards through the backplane and switch fabrics are configured using the CLI.

The 1-Gbps client traffic from a 4-port 1-Gbps/2-Gbps FC aggregation card is compatible with the 8-port FC/GE aggregation card at the other end of the network. Any 1-Gbps FC, FICON, or ISC client signal can be transmitted between a 4-port 1-Gbps/2-Gbps FC aggregation card and an 8-port FC/GE aggregation card.

Figure 5-1 shows an example path of a client signal through the Cisco ONS 15530 and the associated interfaces.

Figure 5-1 Interfaces for a 4-port 1-Gbps/2-Gbps FC Aggregation Card

5.2 Initial Troubleshooting Checklist

Follow this initial checklist before proceeding with the troubleshooting procedures:

- Check that the client receive signal power level is between -18 dBm and -13.5 dBm for multimode SFP optics and between -20 dBm and -3 dBm for single-mode SFP optics. If the receive signal power is not within the range, adjust the attenuation.
- Issue **show interfaces** commands to ensure that the interfaces on the signal path are administratively up and that there are no errors on the interfaces.
- Issue a **show connect** command to verify the status of the cross connections between the 4-port 1-Gbps/2-Gbps FC aggregation card and the ITU trunk card or uplink card.
- Check that the LEDs on the card and SFP optics show the proper state.
- Issue a **show facility-alarm status** command to display the alarms on the interfaces.
- Check that the ITU cards are patched to the correct OADM ports. Issue a **show patch** command to verify that there are no frequency mismatches.
- Before you enable end-to-end speed negotiation, oversubscription, or superportgroup, ensure that the following conditions are met:
 - 4-port 1-Gbps/2-Gbps FC aggregation cards with Functional version 1.20 or later are installed at both ends.
 - The IOS version is 12.2(29)SV or later.
 - 10-Gbps cards with Functional version 2.31 or later are installed.
- Ensure that the configurations at both ends of the link are symmetrical. This is important especially for end-to-end speed negotiation, oversubscription, and superportgroup configurations. Issue the **show running-configuration** command to check the running configuration.
- Ensure that all optical connectors are clean. Refer to the *Cisco ONS 15530 Cleaning Procedures for Fiber Optic Connections* document.

5.3 Troubleshooting 4-Port 1-Gbps/2-Gbps FC Aggregation Card Interface Problems

This section contains troubleshooting procedures for 4-port 1-Gbps/2-Gbps FC aggregation card interface problems.

5.3.1 FC/FICON Encapsulated Twogigabitphy Interface Is Down

Symptom A twogigabitphy interface encapsulated for FC or FICON traffic is down because of Loss of Light.

Table 5-1 describes the potential causes of the symptom and the solutions.

Table 5-1 FC/FICON Encapsulated Twogigabitphy Interface Is Down

Possible Problem	Solution
The SFP optics and the client side optical fiber are different types.	<ol style="list-style-type: none"> 1. Verify that the fiber type, either single-mode or multimode, matches the type of SFP optics installed on the card. 2. Switch to the correct type of fiber if there is a mismatch.
The cabling between the client equipment and the SFP optics are reversed.	Check that the Tx and Rx ports are correctly cabled to the client equipment. If not, then correct the cabling.
The optical fiber between the client equipment and the SFP optics is faulty.	Check the optical fibers connecting the client equipment to the SFP optics. If it they are faulty, replace them.
The connectors on the optical fiber between the client equipment and the SFP optics are dirty.	Refer to the <i>Cisco ONS 15530 Cleaning Procedures for Fiber Optic Connections</i> document.

5.3.2 Twogigabitphy Interface Is Administratively Down

Symptom A twogigabitphy interface is administratively down and cannot carry any type of traffic.

Table 5-2 describes the potential causes of the symptom and the solutions.

Table 5-2 Twogigabitphy Interface Is Administratively Down

Possible Problem	Solution
The SFP optics is not Cisco certified.	<ol style="list-style-type: none"> 1. Issue a show interfaces command for the twogigabitphy interface to verify that the Optical Transceiver field shows “Unknown Vendor.” 2. Replace it with a Cisco certified SFP optics. 3. Issue a no shutdown command on the interface.
The flow identifier is not configured.	<ol style="list-style-type: none"> 1. Issue a show interfaces command for the twogigabitphy interface to verify that the Flow-identifier field contains a valid value. 2. Correct an invalid value with the cdl flow identifier command. 3. Issue a no shutdown command on the interface.
Port group is not configured.	<ol style="list-style-type: none"> 1. Issue a show interfaces command for the twogigabitphy interface to verify that the Portgroup field does not show NULL. 2. Issue the portgroup command to configure a port group. Valid entries range from 0 to 3. 3. Issue a no shutdown command on the interface.

5.3.3 Client Equipment Interface Connected to the 4-Port 1-Gbps/2-Gbps FC Aggregation Card Is Not Up

Symptom The client equipment connected to a twogigabitphy interface is not up.

Table 5-3 describes the potential causes of the symptom and the solutions.

Table 5-3 Client Equipment Connected to a Twogigabitphy Interface Is Not Up

Possible Problem	Solution
The cross connection is not configured.	<ol style="list-style-type: none"> 1. Issue a show interfaces command for the twogigabitphy interface to verify that the Client Laser Status field shows “Down due to Local Condition.” 2. Issue a show connect command to verify the status of the cross connection. 3. Issue the connect command to establish the cross connection.
The client side laser on the 4-port 1-Gbps/2-Gbps FC aggregation card is turned off due to forward laser control activity.	<ol style="list-style-type: none"> 1. Issue a show interfaces command for the remote twogigabitphy interface to check for keepalive timeouts. 2. Issue a show interfaces command for the local twogigabitphy interface to verify that the Client Laser Status field shows “Down due to keep-alive timeout” and that forward laser control is configured. 3. Resolve the problem on the remote twogigabitphy interface.

5.3.4 Client Equipment Detects CVRD Errors

Symptom The client equipment detects CVRD (code violation and running disparity) errors and the twogigabitphy interface shows Loss of Sync.

Table 5-4 describes the potential causes of the symptom and the solutions.

Table 5-4 Client Equipment Detects CVRD Errors

Possible Problem	Solution
The protocol encapsulation configuration is incorrect.	Issue a show interfaces command for the twogigabitphy interface. Issue an encapsulation command if the protocol is incorrect.
The end-to-end speed negotiation configuration is incorrect.	Ensure that the speed of the client devices is set to auto or the same speed is configured on the client devices at both ends. The twogigabitphy interfaces must be locked to the same speed.
Tx CRC errors are reported on the twogigabitphy interface that is connected to an oversubscribed portgroup or superportgroup.	Ensure that the twogigabitphy interface of the 4-port 1-Gbps/2-Gbps FC aggregation card does not generate Tx CRC errors. For more information, refer to the “5.3.13 Oversubscribed Portgroup and Superportgroup Related Problems Are Experienced” section on page 5-10.
The connectors on the optical fiber between the client equipment and the SFP optics are dirty.	Refer to the <i>Cisco ONS 15530 Cleaning Procedures for Fiber Optic Connections</i> document.

5.3.5 Transmit Frame Count Is Not Incrementing

Symptom The Transmit Frame Count field in the **show interfaces** command output for the twogigabitphy interface is not incrementing.

Table 5-5 describes the potential causes of the symptom and the solutions.

Table 5-5 *Transmit Frame Count Is Not Incrementing*

Possible Problem	Solution
An interface in the path is administratively shut down.	<ol style="list-style-type: none"> 1. Issue show interface commands for all interfaces in the signal path, especially on the ITU trunk card or uplink card. 2. Make sure that the interfaces are up and the lasers are on.
The client receive signal power is not strong enough.	<ol style="list-style-type: none"> 1. Verify that the cross connection exists. <ol style="list-style-type: none"> a. Issue a show connect command to verify the status of the cross connection. b. Issue the connect command to establish the cross connection if it is not present. 2. Verify the status of the waveethernetphy interface and the laser on the ITU trunk card. <ol style="list-style-type: none"> a. Issue a show interfaces command for the waveethernetphy interface. b. Issue a no shutdown command if the interface is administratively down. If the interfaces remain down, see Chapter 8, “Troubleshooting 2.5-Gbps ITU Trunk Card Problems,” Chapter 9, “Troubleshooting 10-Gbps ITU Trunk Card Problems,” or Chapter 10, “Troubleshooting 10-Gbps ITU Tunable Trunk Card Problems.” c. Issue a no laser shutdown command if the laser is off.
The cross connection is not properly configured.	<ol style="list-style-type: none"> 1. Issue a show interfaces command to verify that the Client Laser Status field shows “Down due to Local Condition.” 2. Issue a show connect command to verify the status of the cross connection. 3. Issue the connect command to establish the cross connection.
The flow identifier is not configured.	<ol style="list-style-type: none"> 1. Issue a show interfaces command to verify that the Flow-identifier field contains a valid value. 2. Correct an invalid value with the cdl flow identifier command. 3. Issue a no shutdown command on the interface.

5.3.6 FC/FICON Encapsulated Twogigabitphy Interface Receives CRC Errors from Trunk Card

Symptom A twogigabitphy interface encapsulated with either FC or FICON shows CRC (cyclic redundancy check) errors received from the trunk cards. The **show interfaces** command for the interface shows NO TX CRC.

Table 5-6 describes the potential cause of the symptom and the solution.

Table 5-6 *FC/FICON Encapsulated Twogigabitphy Interface Receives CRC Errors from Trunk Card*

Possible Problem	Solution
The transmit buffer is not correctly configured.	<ol style="list-style-type: none"> 1. Issue show controller command for the interface to determine if the BPTX Port Fail register “FIFO EMPTY” has a Current Status as “yes.” If it is, the transmit buffer is not large enough. 2. Issue the tx-buffer size command to increase the buffer size. For information on setting the transmit buffer size on 4-port 1-Gbps/2-Gbps FC aggregation cards, refer to the <i>Cisco ONS 15530 Configuration Guide</i>.
The power of the signal received from the trunk card is close to or below the low warning threshold.	<ol style="list-style-type: none"> 1. Verify that the receive signal power level is between –28 dBm and –8 dBm for a 2.5-Gbps ITU trunk card and between –22 dBm and –6 dBm for a 10-Gbps ITU trunk card and 10-Gbps ITU tunable trunk card. 2. Adjust the attenuation if the signal power is outside the power range for the trunk card.

5.3.7 Both the Local and Remote Twogigabitphy Interfaces Are Down

Symptom The local twogigabitphy interface is down due to a local condition while the remote twogigabitphy interface is down due to a keepalive timeout.

Table 5-7 describes the potential cause of the symptom and the solution.

Table 5-7 *Both the Local and Remote Gigabit Interfaces Are Down*

Possible Problem	Solution
Forward laser control is configured on one interface but not on the other interface.	<ol style="list-style-type: none"> 1. Issue a show interfaces command for both twogigabitphy interfaces to verify the status of the forward laser control configuration. 2. Issue the laser control forward enable command to enable forward laser control on the interface, or the no laser control forward command to disable it.

5.3.8 Twogigabitphy Interface Not Created

Symptom A twogigabitphy interface does not appear in the configuration and is not recognized by the system.

Table 5-8 describes the potential cause of the symptom and the solution.

Table 5-8 Twogigabitphy Interface Not Created

Possible Problem	Solution
Wrong SFP optics is installed.	Issue a show interfaces command for the twogigabitphy interface and verify that the Optical Transceiver field shows a valid value. If not, replace the SFP optics with the correct part.

5.3.9 Twogigabitphy Interface Reports Loss of Sync

Symptom The twogigabitphy interface reports Loss of Sync.

Table 5-9 describes the potential cause of the symptom and the solution.

Table 5-9 Twogigabitphy Interface Reports Loss of Sync

Possible Problem	Solution
End-to-end speed negotiation is not enabled on both the twogigabitphy interfaces in the link.	Enable end-to-end speed negotiation at both the ends.
The twogigabitphy interfaces are not locked to the same speed.	Ensure that the twogigabitphy interfaces are locked to the same speed.
The SFPs do not support the configured speed.	Replace the SFP optics with the correct part.

For more information, refer to the “5.3.13 Oversubscribed Portgroup and Superportgroup Related Problems Are Experienced” section on page 5-10.

5.3.10 Throughput Is Low

Symptom Low throughput is experienced.

Table 5-10 describes the potential cause of the symptom and the solution.

Table 5-10 *Throughput Is Low*

Possible Problem	Solution
After enabling end-to-end speed negotiation, the link has not negotiated to the 2 Gbps speed.	Ensure that the link has negotiated to the 2 Gbps speed.
For oversubscription or superportgroup configurations, flow control is not enabled at both ends.	Ensure that you enable flow control at both ends when oversubscription or superportgroup is configured.
For oversubscription or superportgroup configurations, flow control is not active at both ends.	Ensure that flow control is active at both ends when oversubscription or superportgroup is configured. For more information, refer to the “5.3.12 Flow Control Is Inactive” section on page 5-10.
The subrate and bandwidth lock configurations are not symmetrical at both ends.	Ensure that the subrate and bandwidth lock configurations are symmetrical at both ends.

If the problem persists, verify the throughput after locking the bandwidth at both ends, and then, if possible, after moving the oversubscribed link to a non-oversubscribed link. For more information, refer to the “5.3.13 Oversubscribed Portgroup and Superportgroup Related Problems Are Experienced” section on page 5-10.

5.3.11 Throughput Is Asymmetric

Symptom The throughput in one direction is greater than that in the other direction.

Table 5-11 describes the potential cause of the symptom and the solution.

Table 5-11 *Throughput Is Asymmetric*

Possible Problem	Solution
For superportgroup or oversubscription configurations, the same subrate is not configured on the twogigabitphy interfaces at both ends.	Ensure that the same subrate is configured on the twogigabitphy interfaces at both ends.

5.3.12 Flow Control Is Inactive

Symptom Flow control is not in an active state.

Table 5-12 describes the potential cause of the symptom and the solution.

Table 5-12 *Flow Control Is Inactive*

Possible Problem	Solution
The twogigabitphy interface is administratively down.	Bring up the twogigabitphy interface that is down.
The signal quality of the twogigabitphy interface is bad.	Issue the show interface command to verify the signal quality.
The twogigabitphy interfaces at both ends are not configured to the same speed.	Configure the same speed on the twogigabitphy interfaces at both ends.
Incorrect buffer-to-buffer credits on the client devices connected to the twogigabitphy interfaces.	Ensure that the buffer-to-buffer credit values on the client devices do not exceed 219 for 1 Gbps and 939 for 2 Gbps.

5.3.13 Oversubscribed Portgroup and Superportgroup Related Problems Are Experienced

Symptom Oversubscribed portgroup and superportgroup related problems are experienced.

Table 5-13 describes the potential cause of the symptom and the solution.

Table 5-13 *Oversubscribed Portgroup and Superportgroup Related Problem Are Experienced*

Possible Problem	Solution
Guidelines to configure oversubscription and superportgroup have not been followed.	<ol style="list-style-type: none"> 1. Correct the oversubscription and superportgroup configurations based on the guidelines mentioned in the <i>Cisco ONS 15530 Configuration Guide</i>. 2. Perform a shut/no shut on the twogigabitphy interfaces. If required, perform a shut/no shut on the client interfaces as well.
The oversubscription, subrate, and bandwidth lock configurations at both ends are not the same.	Issue the show running-configuration command to verify the oversubscription configurations at both ends.

Table 5-13 Oversubscribed Portgroup and Superportgroup Related Problem Are Experienced

Possible Problem	Solution
All associated portgroups in a superportgroup are not cross connected.	Issue the show running-configuration command or the show connect command to verify that the associated portgroups are cross connected.
The trunk flow identifiers of the portgroups at both ends do not match.	Issue the show running-configuration command or the show interface superportgroup command to verify the trunk flow identifiers at both ends.
The client devices are not connected to the same twogigabitphy interface or port at both ends.	Ensure that the client devices are connected to the same twogigabitphy interface or port at both ends.
The twogigabitphy interfaces at both ends do not have the same configuration.	Ensure that the twogigabitphy interfaces at both ends have the same configuration. Issue the show running-configuration command or the show interface twogigabitphy command to view the configuration of the twogigabitphy interface.

If the problem persists, continue troubleshooting after locking the bandwidth at both ends, and then, if possible, after moving the oversubscribed link to a non-oversubscribed link.

5.4 Troubleshooting Problems Using show controller Command Output

You can use the **show controllers** command output to determine and resolve problems on your 4-port 1-Gbps/2-Gbps FC aggregation card.

The following example shows the command output for the twogigabitphy interface:

```
Switch# show controllers twogigabitphy 4/0/0
Controller info for interface TwoGigabitPhy4/0/0
Line card base addr: 0x400000
  Optical Transceiver: Single Mode
-----
  BPRX Channel Rx Frame count: 45478467
  BPTX Channel Tx Frame count: 45720664
  BPTX Channel Tx WORD count: 12871348901
-----
TX CRC erro count: 0
QDR CRC error count: 0
QDR PARITY error count: 0

Registers specific to client port 0:
CONEY FPGA base addr: 0x60000
Version.....: 0x6025A27
Reset Control:
  Transmit (no), Receive (no)
Loopback Control:
  Trunk (dis), CTC (dis)
Send Pattern: NOS
```

```

Control & Status:
  Auto Speed: (en), result (2g)
  Login State: (ELP_COMPLETE), Port State: (active)
  Port Encapsulation: (2xFC/FICON)
Port Fail Registers
  (Cause -- UnMasked -- Enable -- Cur Status):
  SFP OIR:          (no) -- (yes) -- (yes) -- (no)
  LINK FAIL:       (yes) -- (yes) -- (yes) -- (no)
  TX FAULT:        (no) -- (yes) -- (yes) -- (no)
  RX DEG:          (no) -- (yes) -- (yes) -- (no)
  LOSS OF LIGHT:   (no) -- (yes) -- (yes) -- (no)
  LOSS OF SYNC:    (no) -- (yes) -- (yes) -- (no)
Laser Control:
  Real Time KATO: (dis) Latched KATO: (en)
  OFC: (dis), BLC: (dis), FLC: (en)
PHY CSR:
  loopback (dis), pre-emphasis (dis)
SFP CSR:
  Present (yes), LOS (no), TXFAULT (no)
  Full Speed (yes), Laser Enabled (yes)
OFC CSR:
  OFC on (no), OFC lineup (no)
  OFC laser ctrl (dis), OFC master (dis), OFC reset (en)
Laser Enable Register:
  Shut reason: RT_KATO(no) LATCH_KATO(no) OFC(no) BLC(no) FLC(no)
  Laser WEN (no), Laser Software Enable (yes)
Backward Laser Control Register
  Real Time Trigger: (no)
  Source: TXFAULT(yes) RXDEG(no) LOL(yes) LOSync(no)
Forward Laser Control Register
  Real Time Trigger: (yes)
  Source: RXDEG(no) LOL(yes) LOSync(no)
Tx LED
  Controlled by hardware (yes), software color (off)
Rx LED
  Controlled by hardware (yes), software color (off)
TX CVRD Error Count: 9, TX CRC Error Count: 3
CVRD Rate Control:
  Threshold: 22149, Time 1000000 usec

BPTX FPGA base addr: 0x50000
Revision.....: 0x5025A30
Registers specific to client port 0:
Memory Sharable: yes, Memory Size(0,1,2): 1
Channel Reset: no
Credit Management:
  en Flow Active: yes
  BP_LOGIN: no, BP_LOGI_DONE: yes, PORT_LOGI_DONE: yes
  EXCESS_CREDIT: no, LOCAL_FLOW: yes, REMOTE_FLOW: yes
  ZERO_CREDIT: no, MEM_L_SIZE: 256, MEM_SIZE: 0x2000
Egress FIFO
  Almost Full Threshold: 6
  Almost Empty Threshold: 4
KeepAlive
  Control: en, Time: 12775(us)
Port Fail Registers
  (Cause -- UnMasked -- Enable -- Cur Status):
  FLOW INACTIVE:   (no) -- (yes) -- (yes) -- (no)
  FIFO FULL:       (no) -- (yes) -- (yes) -- (no)
  FIFO EMPTY:      (no) -- (yes) -- (yes) -- (no)
  BDI-E:           (no) -- (yes) -- (yes) -- (no)
  KeepAlive Timeout: (no) -- (yes) -- (yes) -- (no)
  TxCRC Error:      (no) -- (yes) -- (yes) -- (no)
  EXCESS FRAME:    (no) -- (yes) -- (yes) -- (no)

```

```

ECH TIMEOUT:          (yes) -- (yes) -- (yes) -- (no)
Tx CRC
  Threshold: 18846,   Time: 1000000(us)

BPRX FPGA base addr: 0x40000
  Revision.....: 0x11104
Registers specific to client port 0:
  Channel Reset: no
  Channel CSR:
    2G_Flag: dis,    Port Map: 2,    Port Enable: yes
    Subrate Percentage: 25 %, BW Share: no
  Y-CABLE Register:
    FLC: en,        BDIGEN: dis
  BDI Mask and Control Register:
    Trunk RXF BDI: en, Client RXF BDI: dis, Client TXF BDI: en
    STOP_KA: no,   BDIGENST: no,  BDIEBIT: en,  AS1: 85
  SII: 255
  Flow Control Active to Inactive Transition count: 0
  Flow Control Inactive to Active Transition count: 0
  Oversubscription Available Credits: 944
  Flow Control Available Credits: 944

```

Table 5-14 describes some of the fields in the **show controllers twogigabitphy** command output.

Table 5-14 *show controllers twogigabitphy Command Output Field Descriptions*

Field	Problem Description
FC FIFO egress underflow	Indicates transmit buffer underflow and invalid transmit buffer size.
Tx CRC errors	Indicates GE CRC errors.
Port control	Indicates protocol encapsulation and the status of the Tx and Rx for the port.
Loopback control	Indicates the status of the interface loopback.
FIFO Hi control	Indicates the value for the transmit buffer size in hexadecimal.
External Phy	Indicates if the interface is in sync.
Uplink0 SII register	Indicates the flow identifier value.
Auto speed	Indicates if end-to-end speed negotiation is enabled. The <code>result</code> field displays the negotiated speed.
Subrate percentage	Indicates the percentage of portgroup or superportgroup bandwidth.
BW share	Indicates if the bandwidth is locked.

The following example shows the **show controllers** command output for the superportgroup interface:

```

Switch# show controllers superPortgroup 4/0/0
Controller info for interface SuperPortgroup4/0/0

Line card base addr: 0x400000

-----
          BANDWIDTH                PORT      Trunk Striping
          MAX          -----
Client  RATE  SII  SRATE  SHARE  PC  CRDT_SZ  EN  MAP  Tk0  Tk1  Tk2  Tk3
-----

```

5.4 Troubleshooting Problems Using show controller Command Output

```

Port 2  212  255  187  yes  25  0x2000  yes  2  yes  yes  yes  no
Port 0  212  255  187  no   25  0x2000  yes  2  yes  yes  yes  no
Port 1  212  255  187  yes  25  0x2000  yes  2  yes  yes  yes  no
Port 3  212  255  187  yes  25  0x2000  yes  2  yes  yes  yes  no
-----

-----
Trunk   SII  CPU  OVS  TRUNK  FILLER  DROP  SCRAMBLE
        SHARE  FRAMES  CRC
-----
Port 2  92   0   yes  yes   yes   yes   yes
Port 1  91   0   yes  yes   yes   yes   yes
Port 0  90   0   yes  yes   yes   yes   yes
-----

```

Table 5-15 describes some of the fields in the **show controllers superportgroup** command output.

Table 5-15 *show controllers superportgroup Command Output Field Descriptions*

Field	Problem Description
SII	In the client table, this field indicates the client SII value (255 for superportgroup configurations). In the trunk table, this field indicates the trunk flow identifier (255 for non-superportgroup configurations).
SRATE	Indicates the subrate configured on the twogigabitphy interface (in MBps).
SHARE	Indicates if the bandwidth can be shared with other clients.
PC	Indicates the percentage of the superportgroup or oversubscribed portgroup bandwidth allocated to each twogigabitphy interface.
CRDT_SZ	Indicates the transmit buffer size in hexadecimal (0x2000 for 2-Gbps or auto, and 0x800 for 1-Gbps).
EN	Indicates if the port is hardware enabled.
MAP	Indicates the flow identifier value.
TK0 to TK3	Indicates if superportgroup or trunk sharing is enabled for portgroup0 to portgroup3.
OVS	Indicates if oversubscription is enabled.
Trunk Share	Indicates if trunk sharing is enabled. Trunk sharing must be enabled for superportgroup configurations.
Filler Frames	Indicates if the filler frames are enabled. Filler frames must be enabled for superportgroup configurations.
Drop CRC	Indicates if the CDL frames with CRC errors detected on the portgroup are dropped. Drop CRC must always be enabled.
Scramble	Indicates if scrambling is enabled. Scrambling must be always enabled.

The following example shows the **show controllers** command output for the portgroup interface:

```

Switch# show controllers Portgroup 9/0/1
Controller info for interface Portgroup9/0/1

```

```

Line card base addr: 0x700000
BPTX FPGA base addr: 0x50000
  Revision.....: 0x5025A30
Registers specific to fabric port 1:
  Trunk Reset: no
  QGMII CSR:
    2nd CPU: no, LRCSWEN: yes, Active CPU: 0
    Descrambler: en, CRC Drop: en
  QGMII CVRD
    Threshold: 256, Time: 1000(us)
  Port Fail Registers
    (Cause -- UnMasked -- Enable -- Cur Status):
    CPU0 CVRD: (no) -- (yes) -- (yes) -- (no)
    CPU1 CVRD: (no) -- (yes) -- (yes) -- (no)

BPRX FPGA base addr: 0x40000
  Revision.....: 0x11104

Registers specific to fabric port 1:
  Trunk Reset: no
  Trunk Loopback: dis
  QGMII CSR:
    Scrambler: en Oversub: en
    Trunk Sharing: dis Filler Frames: dis
  Trunk SII: 255 (Mib SII: 255)

CHANNEL: 1
-----
BPTX SII LUT 0x752400:
0091 00000200
0092 00000400

-----

```

Client	BANDWIDTH					PORT		
	MAX RATE	SII	SRATE	SHARE	PC	CRDT_SZ	EN	MAP
Port 1	106	91	100	no	40	0x800	yes	1
Port 2	212	92	150	no	60	0x2000	yes	1

Table 5-16 describes some of the fields in the **show controllers portgroup** command output.

Table 5-16 *show controllers portgroup Command Output Field Descriptions*

Field	Problem Description
Oversub	Indicates if oversubscription is enabled in the Cisco ONS 15530 hardware. This field must contain <code>en</code> for an oversubscribed portgroup and <code>dis</code> for a non-oversubscribed portgroup.
Trunk Sharing	Indicates if trunk sharing is enabled. Trunk sharing must be enabled for superportgroup configurations, and disabled for other oversubscribed portgroup configurations.
Filler Frames	Indicates if the filler frames are enabled. Filler frames must be enabled for superportgroup configurations, and disabled for other oversubscribed portgroup configurations.

Table 5-16 *show controllers portgroup Command Output Field Descriptions (continued)*

Field	Problem Description
Trunk SII	Indicates the trunk flow identifier. This field will contain the trunk flow identifier for superportgroup configurations, and 255 for other oversubscribed portgroup configurations.
BPTX SII LUT	Indicates the cdl flow identifier of the twogigabitphy interfaces connected to the portgroup. This field can contain the values, 100, 200, 400, and 800, which refer to port0, port1, port2, and port3 respectively.
MAP	Indicates that the twogigabitphy interfaces are mapped to the specified portgroup.

5.5 Troubleshooting 4-Port 1-Gbps/2-Gbps FC Aggregation Card Problems Using Loopbacks

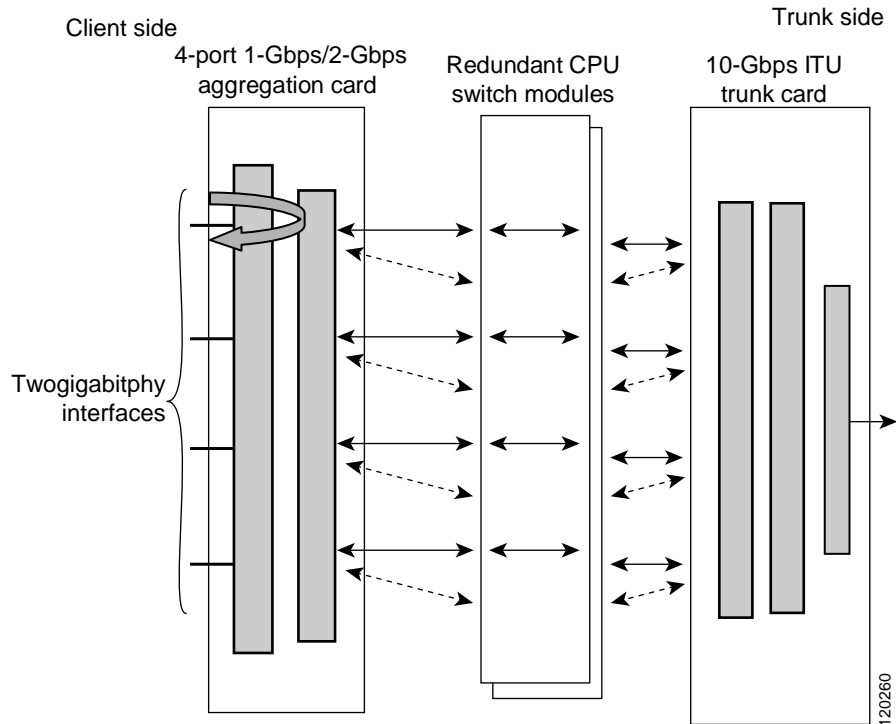
This section describes how to use software loopbacks to perform fault isolation for signals on 4-port 1-Gbps/2-Gbps FC aggregation cards. The 4-port 1-Gbps/2-Gbps FC aggregation card supports two types of software loopbacks:

- Facility loopbacks
- Terminal loopbacks

To perform further loopback operations, see the “8.4 Troubleshooting 2.5-Gbps ITU Trunk Card Problems Using Loopbacks” section on page 8-5, the “9.4 Troubleshooting 10-Gbps ITU Trunk Card Problems Using Loopbacks” section on page 9-5, and the “10.4 Troubleshooting 10-Gbps ITU Tunable Trunk Card Problems Using Loopbacks” section on page 10-6.

5.5.1 Facility Loopbacks

Facility loopbacks on 4-port 1-Gbps/2-Gbps FC aggregation cards verify the functioning of the SFP optics from the client side (see Figure 5-2).

Figure 5-2 Facility Loopback Example

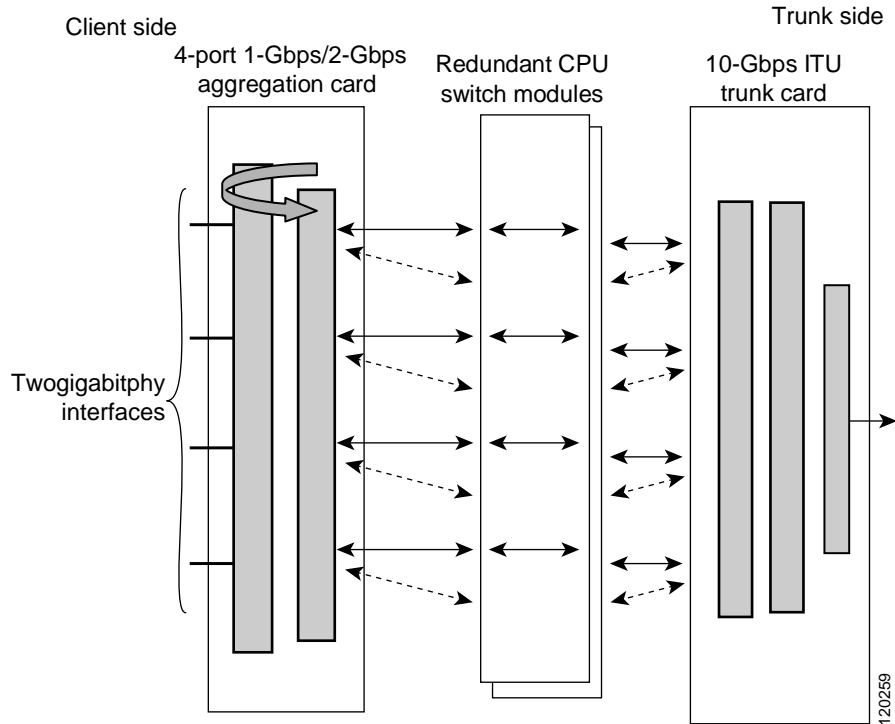
Procedure: Create a Facility Loopback

-
- Step 1** Issue a **loopback facility** command on the twogigabitphy interface.
 - Step 2** Check that the traffic is reaching the client equipment.
 - Step 3** If the signal does not reach the client equipment, replace the SFP optics.
-

5.5.2 Terminal Loopbacks

Terminal loopbacks verify the functioning of the 4-port 1-Gbps/2-Gbps FC aggregation cards from the trunk side (see Figure 5-3).

Figure 5-3 Terminal Loopback Example



Procedure: Create a Terminal Loopback

-
- Step 1** Issue a **loopback terminal** command on the twogigabitphy interface.
 - Step 2** Check that the traffic is reaching the client equipment.
 - Step 3** If the signal does not reach the far end, check the trunk fiber and the interfaces along the signal path. If the fiber is intact, replace the card.
-



Troubleshooting 8-Port FC/GE Aggregation Card Problems

This chapter describes how to troubleshoot 8-port FC/GE aggregation card interface problems. This chapter includes the following sections:

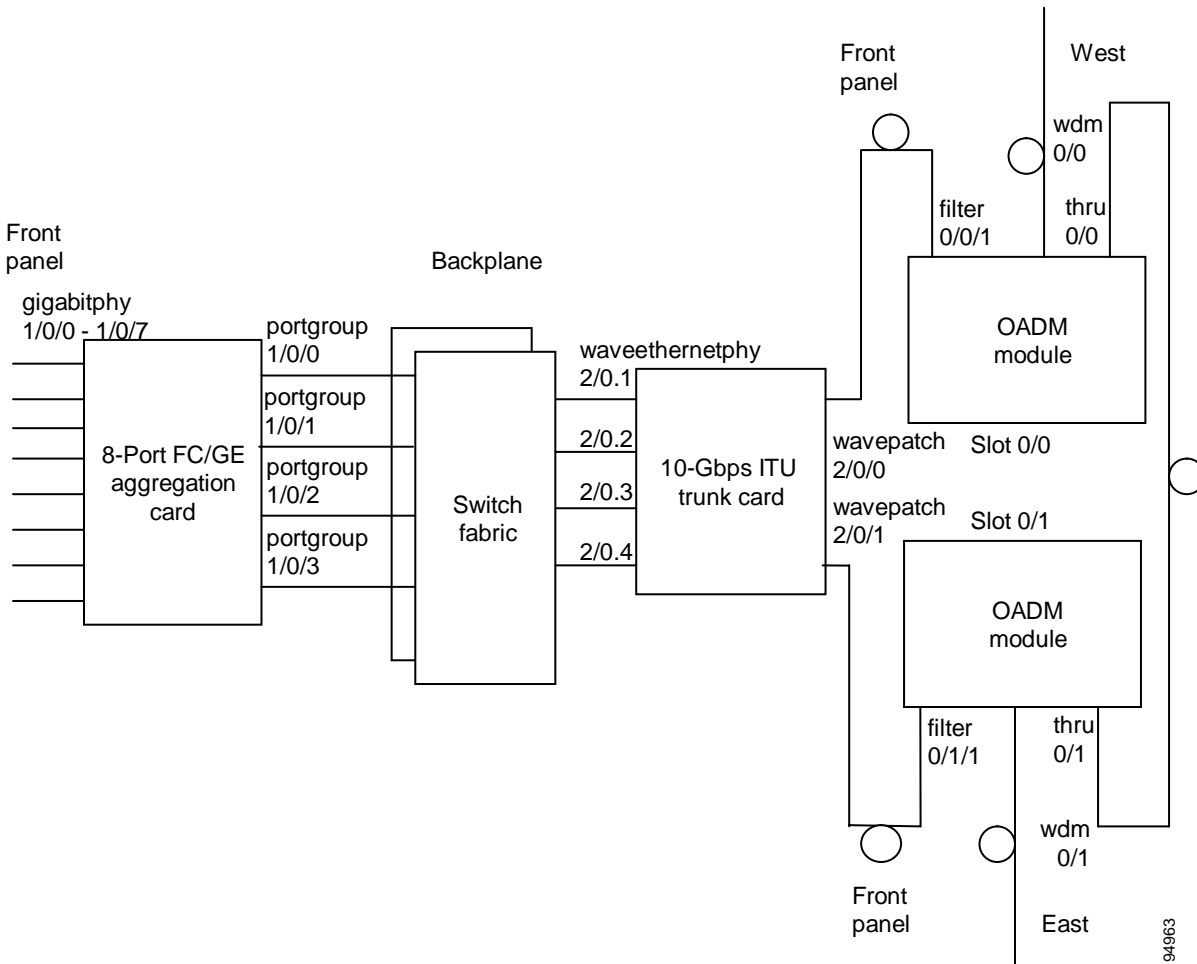
- 6.1 Overview, page 6-1
- 6.2 Initial Troubleshooting Checklist, page 6-2
- 6.3 Troubleshooting 8-Port FC/GE Aggregation Card Interface Problems, page 6-3
- 6.5 Troubleshooting 8-Port FC/GE Aggregation Card Problems Using Loopbacks, page 6-11

6.1 Overview

The 8-port FC/GE aggregation card uses SFP (small form-factor pluggable) optical transceivers to provide up to eight configurable client interfaces. Each interface can be configured in the CLI (command-line interface) for FC (Fibre Channel), FICON (fiber connection), or GE (Gigabit Ethernet) traffic.

Figure 6-1 shows an example path of a client signal through the Cisco ONS 15530 and the associated interfaces.

Figure 6-1 Interfaces for an 8-Port FC/GE Aggregation Card



6.2 Initial Troubleshooting Checklist

Follow this initial checklist before proceeding with the troubleshooting procedures:

- Check that the client receive signal power level is between -18 dBm and -13.5 dBm for multimode SFP optics and between -20 dBm and -3 dBm for single-mode SFP optics. If the receive signal power is not within the range, adjust the attenuation.
- Issue **show interfaces** commands to ensure that the interfaces on the signal path are administratively up and that there are no errors on the interfaces.
- Issue a **show connect** command to verify the status of the cross connections between the 8-port FC/GE aggregation card and the ITU trunk card or uplink card.
- Check that the LEDs on the card and SFP optics show the proper state.
- Issue a **show facility-alarm status** command to display the alarms on the interfaces.
- Check that the ITU cards are patched to the correct OADM ports. Issue a **show patch** command to verify that there are no frequency mismatches.

- Ensure that all optical connectors are clean. Refer to the *Cisco ONS 15530 Cleaning Procedures for Fiber Optic Connections* document.

6.3 Troubleshooting 8-Port FC/GE Aggregation Card Interface Problems

This section contains troubleshooting procedures for 8-port FC/GE aggregation card interface problems.

6.3.1 FC/FICON Encapsulated Gigabitphy Interface Is Down

Symptom A gigabitphy interface encapsulated for FC or FICON traffic is down because of Loss of Light. Table 6-1 describes the potential causes of the symptom and the solutions.

Table 6-1 FC/FICON Encapsulated Gigabitphy Interface Is Down

Possible Problem	Solution
The SFP optics and the client side optical fiber are different types.	<ol style="list-style-type: none"> 1. Verify that the fiber type, either single-mode or multimode, matches the type of SFP optics installed on the card. 2. Switch to the correct type of fiber if there is a mismatch.
The cabling between the client equipment and the SFP optics are reversed.	Check that the Tx and Rx ports are correctly cabled to the client equipment. If not, then correct the cabling.
The optical fiber between the client equipment and the SFP optics is faulty.	Check the optical fibers connecting the client equipment to the SFP optics. If it they are faulty, replace them.
The connectors on the optical fiber between the client equipment and the SFP optics are dirty.	Refer to the <i>Cisco ONS 15530 Cleaning Procedures for Fiber Optic Connections</i> document.

6.3.2 GE Encapsulated Gigabitphy Interface Is Down

Symptom A gigabitphy interface encapsulated for GE traffic is down because of Loss of Light or Loss of Sync.

Table 6-2 describes the potential causes of the symptom and the solutions.

Table 6-2 GE Encapsulated Gigabitphy Interface Is Down

Possible Problem	Solution
The SFP optics and the client side optical fiber are different types.	<ol style="list-style-type: none"> 1. Verify that the fiber type, either single-mode or multimode, matches the type of SFP optics installed on the card. 2. Switch to the correct type of fiber if there is a mismatch.
The cabling between the client equipment and the SFP optics are reversed.	Check that the Tx and Rx ports are correctly cabled to the client equipment. If not, then correct the cabling.
The optical fiber between the client equipment and the SFP optics is faulty.	Check the optical fibers connecting the client equipment to the SFP optics. If it they are faulty, replace them.
The connectors on the optical fiber between the client equipment and the SFP optics are dirty.	Refer to the <i>Cisco ONS 15530 Cleaning Procedures for Fiber Optic Connections</i> document.
Autonegotiation is enabled on the client equipment.	<ol style="list-style-type: none"> 1. Disable autonegotiation on the client equipment. 2. Upgrade the functional image on the 8-port FC/GE aggregation card to version 2.30 and the Cisco IOS release to 12.2(18)SV or later. <p>Note Functional image versions earlier than 2.27 do not support autonegotiation. Functional image versions between 2.27 and 2.3 support autonegotiation, but not end-to-end autonegotiation. Functional image version 2.3 and above support end-to-end autonegotiation. Link defects such as a broken fiber from the FC/GE card to the client device at one end are not propagated to the client at the other end.</p>

6.3.3 Gigabitphy Interface Is Administratively Down

Symptom A gigabitphy interface is administratively down and cannot carry any type of traffic.

Table 6-3 describes the potential causes of the symptom and the solutions.

Table 6-3 *Gigabitphy Interface Is Administratively Down*

Possible Problem	Solution
The SFP optics is not Cisco certified.	<ol style="list-style-type: none"> 1. Issue a show interfaces command for the gigabitphy interface to verify that the Optical Transceiver field shows “Unknown Vendor.” 2. Replace it with a Cisco certified SFP optics. 3. Issue a no shutdown command on the interface.
The flow identifier is not configured.	<ol style="list-style-type: none"> 1. Issue a show interfaces command for the gigabitphy interface to verify that the Flow-identifier field contains a valid value. 2. Correct an invalid value with the cdl flow identifier command. 3. Issue a no shutdown command on the interface.

6.3.4 Client Equipment Interface Connected to the 8-Port FC/GE Aggregation Card Is Not Up

Symptom The client signal to one gigabitphy interface fell below an alarm threshold falls below an alarm threshold value.

Table 6-4 describes the potential causes of the symptom and the solutions.

Table 6-4 *Client Equipment Interface Connected to the 8-Port FC/GE Aggregation Card Is Not Up*

Possible Problem	Solution
The cross connection is not configured.	<ol style="list-style-type: none"> 1. Issue a show interfaces command for the gigabitphy interface to verify that the Client Laser Status field shows “Down due to Local Condition.” 2. Issue a show connect command to verify the status of the cross connection. 3. Issue the connect command to establish the cross connection.
The client side laser on the 8-port FC/GE aggregation card is turned off due to forward laser control activity.	<ol style="list-style-type: none"> 1. Issue a show interfaces command for the remote gigabitphy interface to check for keepalive timeouts. 2. Issue a show interfaces command for the local gigabitphy interface to verify that the Client Laser Status field shows “Down due to keep-alive timeout” and that forward laser control is configured. 3. Resolve the problem on the remote gigabitphy interface.

6.3.5 Client Equipment Detects CVRD Errors

Symptom The client equipment detects CVRD (code violation and running disparity) errors and the gigabitphy interface shows Loss of Sync.

Table 6-5 describes the potential causes of the symptom and the solutions.

Table 6-5 Client Equipment Detects CVRD Errors

Possible Problem	Solution
The protocol encapsulation configuration is incorrect.	Issue a show interfaces command for the gigabitphy interface. Issue an encapsulation command if the protocol is incorrect.
The connectors on the optical fiber between the client equipment and the SFP optics are dirty.	Refer to the <i>Cisco ONS 15530 Cleaning Procedures for Fiber Optic Connections</i> document.
Autonegotiation is enabled on the client equipment.	Disable autonegotiation on the client equipment. Note The 8-port FC/GE aggregation card does not support autonegotiation for GE traffic.

6.3.6 Transmit Frame Count Is Not Incrementing

Symptom The Transmit Frame Count field in the **show interfaces** command output for the gigabitphy interface is not incrementing.

Table 6-6 describes the potential causes of the symptom and the solutions.

Table 6-6 Transmit Frame Count Is Not Incrementing

Possible Problem	Solution
An interface in the path is administratively shut down.	<ol style="list-style-type: none"> Issue show interface commands for all interfaces in the signal path, especially on the ITU trunk card or uplink card. Make sure that the interfaces are up and the lasers are on.
The client receive signal power is not strong enough.	<ol style="list-style-type: none"> Verify that the cross connection exists. <ol style="list-style-type: none"> Issue a show connect command to verify the status of the cross connection. Issue the connect command to establish the cross connection if it is not present. Verify the status of the waveethernetphy interface and the laser on the ITU trunk card. <ol style="list-style-type: none"> Issue a show interfaces command for the waveethernetphy interface. Issue a no shutdown command if the interface is administratively down. If the interfaces remain down, see Chapter 8, “Troubleshooting 2.5-Gbps ITU Trunk Card Problems,” Chapter 9, “Troubleshooting 10-Gbps ITU Trunk Card Problems,” or Chapter 10, “Troubleshooting 10-Gbps ITU Tunable Trunk Card Problems.” Issue a no laser shutdown command if the laser is off.

Table 6-6 Transmit Frame Count Is Not Incrementing (continued)

Possible Problem	Solution
The cross connection is not properly configured.	<ol style="list-style-type: none"> 1. Issue a show interfaces command to verify that the Client Laser Status field shows “Down due to Local Condition.” 2. Issue a show connect command to verify the status of the cross connection. 3. Issue the connect command to establish the cross connection.
The flow identifier is not configured.	<ol style="list-style-type: none"> 1. Issue a show interfaces command to verify that the Flow-identifier field contains a valid value. 2. Correct an invalid value with the cdl flow identifier command. 3. Issue a no shutdown command on the interface.

6.3.7 Local Interface with GE Encapsulation Receives Frames But Not the Remote Interface

Symptom A gigabitphy interface on the local system receives frames but the remote interface does not receive any frames.

Table 6-7 describes the potential causes of the symptom and the solutions.

Table 6-7 Local Interface With GE Encapsulation Receives Frames But Not the Remote Interface

Possible Problem	Solution
The frame size of the GE traffic is too large.	Issue a show interfaces command for the gigabitphy interface to verify whether the Giant Packets field and Runt Packet field are incrementing. If they are, the signal contains traffic that the Cisco ONS 15530 does not support. The maximum frame size supported by is 10232 bytes.
The flow identifier is not configured correctly.	<ol style="list-style-type: none"> 1. Issue a show interfaces command for both the local and remote gigabitphy interfaces to verify that the Flow-identifier field contains a correct value. Both the local and remote interfaces must have the same value. 2. Correct an incorrect value with the cdl flow identifier command. 3. Issue a no shutdown command on the interface.

6.3.8 FC/FICON Encapsulated Gigabitphy Interface Receives CRC Errors from Trunk Card

Symptom A gigabitphy interface encapsulated with either FC or FICON shows CRC (cyclic redundancy check) errors received from the trunk cards. The **show interfaces** command for the interface shows NO TX CRC.

Table 6-8 describes the potential cause of the symptom and the solution.

Table 6-8 *FC/FICON Encapsulated Gigabitphy Interface Receives CRC Errors from Line Card*

Possible Problem	Solution
The transmit buffer is not correctly configured.	<ol style="list-style-type: none"> 1. Issue show controller command for the interface to determine if the FC Egress FIFO Underflow field is incrementing. If it is, the transmit buffer is not large enough. 2. Issue the tx-buffer size command to increase the buffer size. For information on setting the transmit buffer size on 8-port FC/GE aggregation card, refer to the <i>Cisco ONS 15530 Configuration Guide</i>.
The power of the signal received from the trunk card is close to or below the low warning threshold.	<ol style="list-style-type: none"> 1. Verify that the receive signal power level is between -28 dBm and -8 dBm for a 2.5-Gbps ITU trunk card and between -22 dBm and -6 dBm for a 10-Gbps ITU trunk card. 2. Adjust the attenuation if the signal power is outside the power range for the trunk card.

6.3.9 Both the Local and Remote Gigabit Interfaces Are Down

Symptom The local gigabitphy interface is down due to a local condition while the remote gigabitphy interface is down and the remote gigabitphy interface is down due to a keepalive timeout.

Table 6-9 describes the potential cause of the symptom and the solution.

Table 6-9 *Both the Local and Remote Gigabit Interfaces Are Down*

Possible Problem	Solution
Forward laser control is configured on one interface but not on the other interface.	<ol style="list-style-type: none"> 1. Issue a show interfaces command for both gigabitphy interfaces to verify the status of the forward laser control configuration. 2. Issue the laser control forward enable command to enable forward laser control on the interface or the no laser control forward command to disable it.

6.3.10 Gigabitphy Interface Not Created

Symptom A gigabitphy interface does not appear in the configuration and the system does not recognize it.

Table 6-10 describes the potential cause of the symptom and the solution.

Table 6-10 *Gigabitphy interface not created*

Possible Problem	Solution
Wrong SFP optics is installed.	Issue a show interfaces command for the gigabitphy interface and verify that the Optical Transceiver field shows a valid value. If not, replace the SFP optics with the correct part.

6.4 Debugging Problems Using show controller Command Output

You can use the **show controllers** command output to determine and resolve problems on your 8-port FC/GE aggregation card. The following is an example of the command output:

```
Switch# show controllers gigabitphy 4/0/2
Line card base addr: 0x400000
  Optical Transceiver: Multi-Mode
  FC Egress FIFO Underflow: 0
  FC Egress FIFO Overflow: 0
  Uplink Request FIFO full: 0
  Uplink Data FIFO full: 0
  Downlink Descriptor FIFO full: 0
  Downlink Data FIFO full: 0
  Tx CRC errors: 0
Registers specific to fabric port 2:
Encapsulation FPGA 0 base addr: 0x80000
Version.....: 0x50410621
ID.....: 0x40000
Port Control:
  Line interface type.....: GigabitEthernet
  Line port transmit.....: enabled
  Line port receive.....: enabled
Port Control 1.....: 0x960
Loopback Control:
  Gigabit interface loopback.....: disabled
  Line interface loopback.....: disabled
Port State.....: 0x0
  FC interface.....: active
Port Fail Cause.....: 0x11
  Loss Of sync.....: yes
  Loss Of signal.....: no
  Receive degrade.....: no
  Transmit fault.....: no
  Inactive inflow control mode.....: yes
  Egress fifo full.....: no
  Transceiver present.....: no
Port Fail Mask.....: 0x3F
  Loss Of sync.....: yes
  Loss Of signal.....: yes
  Receive degrade.....: yes
  Transmit fault.....: yes
  Inactive in flow control mode.....: yes
  Egress fifo full.....: yes
  Transceiver present.....: no
Port Fail Status.....: 0xE2
  Loss Of signal from xcvr.....: no
  Loss Of signal from phy.....: yes
  Egress fifo full.....: no
  Transmit fault from phy.....: no
  Transceiver present.....: no
  Loss of sync.....: yes
  Inactive.....: yes
  Egress fifo empty.....: yes
Port Fail Status Mask...: 0xF6
  Loss Of signal from xcvr.....: no
  Loss Of signal from phy.....: yes
  Receive degrade.....: yes
  Transmit fault from phy.....: no
  Transceiver present.....: yes
```

```

    Loss of sync.....: yes
Reset Register.....: 0xFF00
Ordered-Set Control.....: 0x0
Credit Mgmt Control:
    Credit memory size.....: 0x800
    Port login mode enable.....: yes
    Flow control enable.....: no
Credit Mgmt Status:
    Hudson Login Complete.....: no
    Client Login Complete.....: no
    Excess Credit Detect.....: no
    Flow Control Active.....: no
Indirect Address.....: 0x8130007F
Indirect Data.....: 0x11
FC Port 2 Source ID.....: 0x0
FIFO Hi Control.....: 0x4
FIFO Low Control.....: 0x2
OFC Control.....: 0x8400C3
PHY Control:
    External phy loopback.....: disabled
    External phy.....: locked
    External phy byte sync.....: no
    External phy internal byte sync.....: enabled
Transceiver Control:
    Auto laser shut.....: disabled
    Transceiver bandwidth.....: full
    Laser shut control for simi interface: enabled
    Transceiver.....: present
Laser Control:
    External transceiver transmit.....: disabled
    Write for ext transceiver tx enable: disabled
    External transceiver transmit.....: OFF
    Hardware FLC.....: disabled
Clock Control.....: 0x0
Mux/Demux FPGA 0 base addr: 0x40000
Registers specific to client port 2:
    Uplink0 SII Register....: 0xFF (255)
    GE0 MTU.....: 0x27F80040
    GE0 Tx CRC Threshold....: 0x64

```

Table 6-11 describes some of the fields in the **show controllers** command output that are very useful.

Table 6-11 *show controllers Command Output Field Descriptions*

Field	Problem Description
FC FIFO Egress Underflow	Indicates transmit buffer underflow and invalid transmit buffer size.
Tx CRC Errors	Indicates GE CRC errors.
Port Control:	Indicates protocol encapsulation and the status of the Tx and Rx for the port.
Loopback Control:	Indicates the status of the interface loopback.
FIFO Hi Control	Indicates the value for the transmit buffer size in hexadecimal.
External Phy	Indicates if the interface is in sync.
Uplink0 SII Register	Indicates the flow identifier value.

6.5 Troubleshooting 8-Port FC/GE Aggregation Card Problems Using Loopbacks

This section describes how to use software loopbacks to perform fault isolation for signals on 8-port FC/GE aggregation cards. The 8-port FC/GE aggregation card supports two types of software loopbacks:

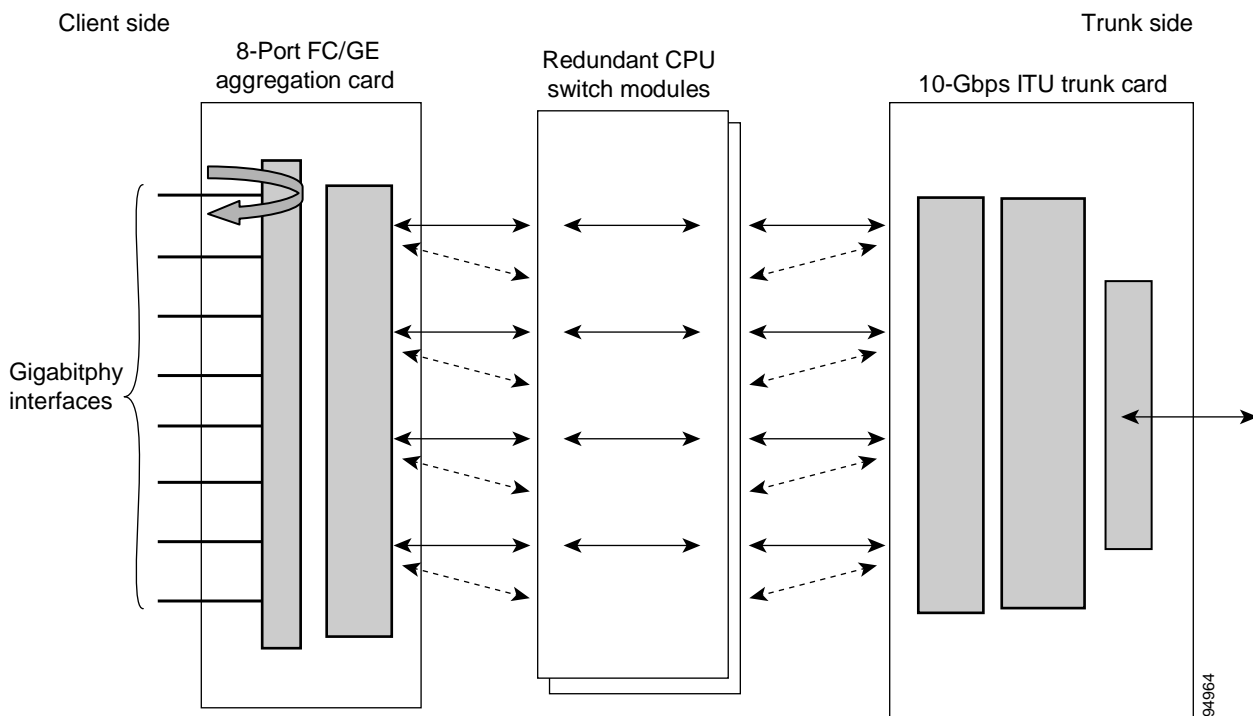
- Facility loopbacks
- Terminal loopbacks

To perform further loopback operations, see the “8.4 Troubleshooting 2.5-Gbps ITU Trunk Card Problems Using Loopbacks” section on page 8-5, the “9.4 Troubleshooting 10-Gbps ITU Trunk Card Problems Using Loopbacks” section on page 9-5, and the “10.4 Troubleshooting 10-Gbps ITU Tunable Trunk Card Problems Using Loopbacks” section on page 10-6.

6.5.1 Facility Loopbacks

Facility loopbacks on 8-port FC/GE aggregation cards verify the functioning of the SFP optics from the client side (see Figure 6-2).

Figure 6-2 Facility Loopback Example



To create a facility loopback:

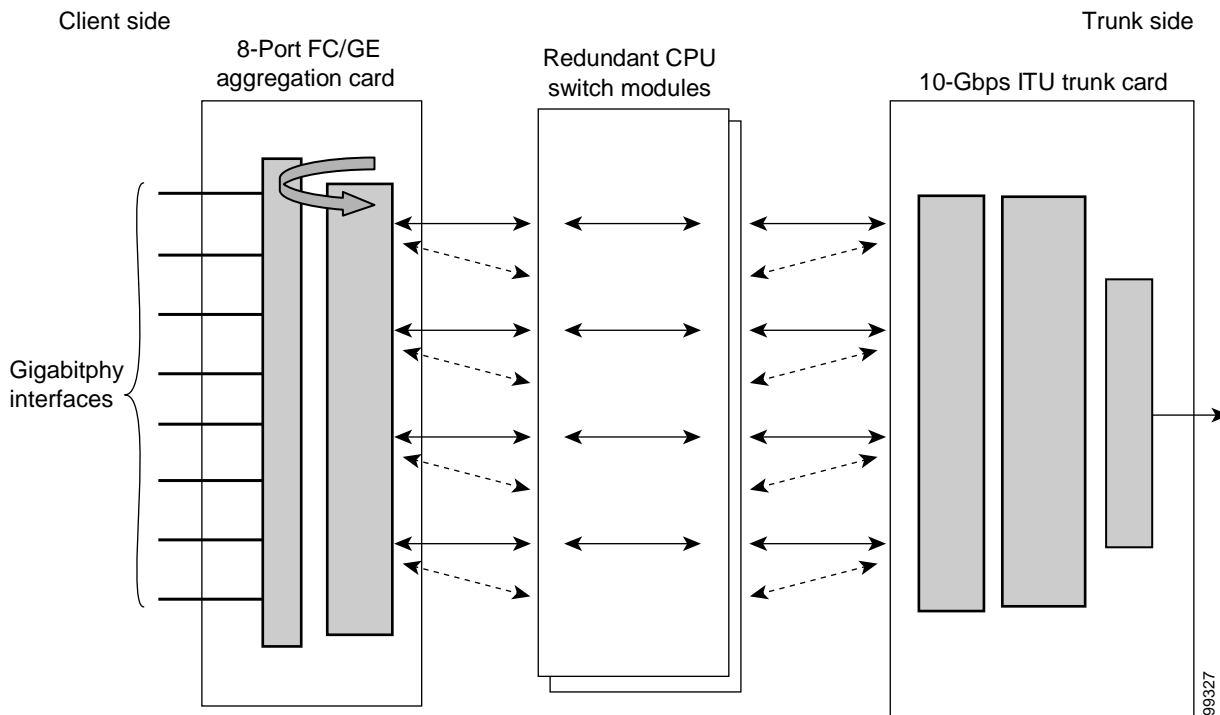
- Step 1** Issue a **loopback facility** command on the gigabitphy interface.
- Step 2** Check that the traffic is reaching the client equipment.

Step 3 If the signal does not reach the client equipment, replace the SFP optics.

6.5.2 Terminal Loopbacks

Terminal loopbacks verify the functioning of the 8-port FC/GE aggregation cards from the trunk side (see Figure 6-3).

Figure 6-3 Terminal Loopback Example



To create a terminal loopback:

- Step 1** Issue a **loopback terminal** command on the gigabitPHY interface.
- Step 2** Check that the traffic is reaching the client equipment.
- Step 3** If the signal does not reach the far end, check the trunk fiber and the interfaces along the signal path. If the fiber is intact, replace the card.



Troubleshooting 8-Port Multi-Service Muxponder Problems

This chapter describes how to troubleshoot 8-port multi-service muxponder problems. This chapter includes the following sections:

- 7.1 Overview, page 7-1
- 7.2 Initial Troubleshooting Checklist, page 7-2
- 7.3 Troubleshooting Multirate Interface Problems, page 7-2
- 7.4 Troubleshooting Trunk-Side Interfaces, page 7-7
- 7.5 Troubleshooting TSI Protocol Problems, page 7-9
- 7.6 Troubleshooting 8-Port Multi-Service Muxponder Problems Using Loopbacks, page 7-10

7.1 Overview

The 8-port multi-service muxponder aggregates up to eight ports of client traffic into a 2.5-Gbps DWDM trunk circuit. The muxponder transports a mix of different protocols among sites in a metropolitan DWDM network. The protocols that can be aggregated and transported range from high-speed services such as Fibre Channel and Gigabit Ethernet to low-speed services such as OC-3, Fast Ethernet, or even T1 or E1.

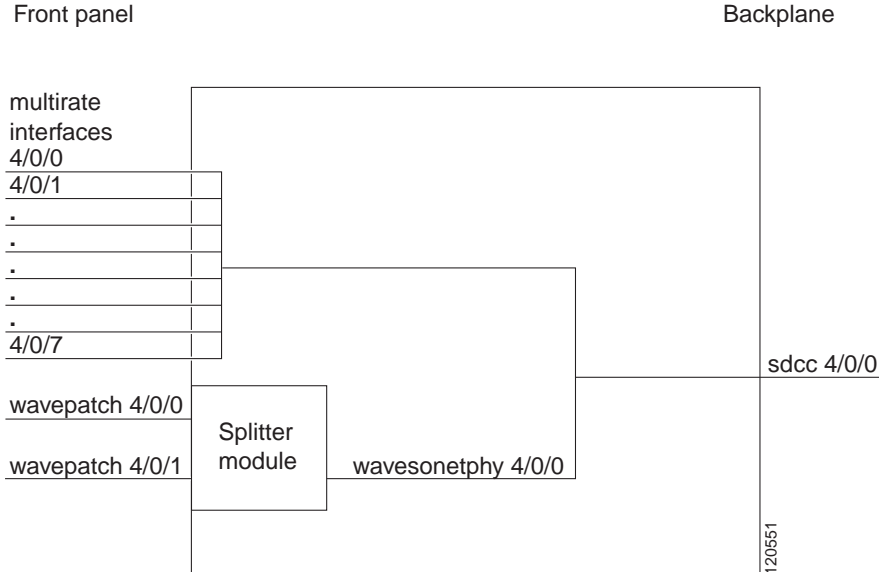
The 8-port multi-service muxponder uses SFPs for the client signals. There are no restrictions on populating the line card with SFPs. For example, you can mix a single-mode SFP with a multimode SFP on the same muxponder.

Figure 7-1 shows the interfaces of the 8-port multi-service muxponder.



Note

Although the 8-port multi-service muxponder uses a SONET-like framing structure to aggregate multiple client data streams, it is not SONET compliant on the optical trunk output. The muxponder ITU compliant optical trunk output must be used in an end-to-end configuration and cannot be connected to a SONET/SDH OADM.

Figure 7-1 8-Port Multi-Service Muxponder Interfaces (Splitter Shown)

7.2 Initial Troubleshooting Checklist

Follow this initial checklist before proceeding with the troubleshooting procedures:

- Ensure the trunk laser is not shut down on the wavesonetphy interface, and that the laser frequency is correctly configured.
- Ensure that TSI (time slot interface) mapping is enabled on the wavesonetphy interfaces.
- Ensure that the sdcc interface is administratively up.
- Issue the **show interfaces** command to ensure the multirate, wavesonetphy, wavepatch, and sdcc interfaces are administratively up and all interfaces on the signal path are administratively up, with no errors. Ensure the trunk receive power level is within the valid range (-28 to -8 dBm).
- Issue the **show tsi** command to ensure that the TSI mapping is correct.
- Ensure that the 8-port multi-service muxponder LEDs are in the proper state.
- Issue a **show facility-alarm status** command to display the alarms on the interfaces.
- Ensure the 8-port multi-service muxponders are patched to the correct OADM ports. Issue the **show patch** command to verify there are no frequency mismatches.
- Ensure that all optical connectors are clean. Refer to the *Cisco ONS 15530 Cleaning Procedures for Fiber Optic Connections* document.

7.3 Troubleshooting Multirate Interface Problems

This section contains troubleshooting procedures for multirate interface problems on the 8-port multi-service muxponder.

7.3.1 Loss of Light on Multirate Interfaces

Symptom A multirate interface encapsulated for optical Gigabit Ethernet, FC, FICON, ESCON, optical Fast Ethernet, SONET OC-3, SDH STM-1 or ITS is down due to Loss of Light.

Table 7-1 describes the potential causes of the symptom and the solutions.

Table 7-1 *Multirate Interface Is Down Due to Loss of Light*

Possible Problem	Solution
Wrong cable type is used.	Verify that the connected fiber type (SM/MM) is the same as that supported by the SFP on the multirate interface.
Cabling between the client equipment and the SFP is incorrect.	Verify that the transmit and receive cables are correctly installed.
Incoming power level is low.	Use a power meter to check the receive power level to the multirate interface. Adjust attenuation as needed.
Optical connectors are dirty.	Check the optical connections between the client equipment and the SFP for dirt, bends, or breaks. Clean or replace as necessary. Refer to the <i>Cisco ONS 15530 Cleaning Procedures for Fiber Optic Connections</i> document.

7.3.2 Loss of Sync on Multirate Interfaces

Symptom A multirate interface encapsulated for optical Gigabit Ethernet, FC, FICON, ESCON or DVB-ASI (Digital Video Broadcast-Asynchronous Serial Interface) is down due to Loss of Sync.

Table 7-2 describes the potential causes of the symptom and the solutions.

Table 7-2 *Multirate Interface Is Down Due to Loss of Sync*

Possible Problem	Solution
Interface improperly configured or incorrect protocol.	Issue the show interfaces multirate command to verify that the correct protocol is configured.
Optical connectors are dirty.	Check the optical connections between the client equipment and the SFP for dirt, bends, or breaks. Clean or replace as necessary. Refer to the <i>Cisco ONS 15530 Cleaning Procedures for Fiber Optic Connections</i> document.

7.3.3 Loss of Lock on Multirate Interfaces

Symptom A multirate interface encapsulated for optical Gigabit Ethernet, FC, FICON, ESCON, optical Fast Ethernet, SONET OC-3, SDH STM-1 or ITS is down due to Loss of Lock.

Table 7-3 describes the potential causes of the symptom and the solutions.

Table 7-3 *Multirate Interface Is Down Due to Loss of Lock*

Possible Problem	Solution
Incorrect protocol.	Issue a show interfaces multirate command to verify that the correct protocol is configured.
Optical connectors are dirty.	Check the optical connections between the client equipment and the SFP for dirt, bends, or breaks. Clean or replace as necessary. Refer to the <i>Cisco ONS 15530 Cleaning Procedures for Fiber Optic Connections</i> document.

7.3.4 Loss of Signal on Multirate Interfaces

Symptom A multirate interface encapsulated for DVB-ASI, copper Gigabit Ethernet, copper Fast Ethernet, SDI, T1, or E1 is down due to Loss of Signal.

Table 7-4 describes the potential causes of the symptom and the solutions.

Table 7-4 *Multirate Interface Down Due to Loss of Signal*

Possible Problem	Solution
Incorrect cable connection or wrong cable is used.	Ensure that the cable is connected. Also confirm that the pin outs are right for the cable connectors.
Line coding mismatch.	Ensure that the client equipment is configured as HDB3 for E1 or B8ZS for T1.
Auto negotiation mismatch between the multirate interface and the client interface.	For multirate interfaces encapsulated for copper Gigabit Ethernet or copper Fast Ethernet, ensure that the auto negotiation setting is the same as that of the connected client interface, either on or off.

7.3.5 AIS Error on Multirate Interface Encapsulated for T1 or E1

Symptom AIS (alarm Indication signal) errors on a multirate interface encapsulated for T1 or E1.

Table 7-5 describes the potential cause of the symptom and the solution.

Table 7-5 AIS Errors on a Multirate Interface

Possible Problem	Solution
Connected client interface is sending AIS errors.	The client interface connected to the multirate interface may be shut down. Enable the client interface.

7.3.6 Multirate Interface Displays Remote Client Error Message

Symptom The show interface multirate command output displays a “remote client error” message..

Table 7-6 describes the potential causes of the symptom and the solutions.

Table 7-6 Multirate Interface Displays “Remote Client Error” Message

Possible Problem	Solution
Data receive error from remote client.	<ol style="list-style-type: none"> 1. Issue a show interfaces multirate command to the local multirate interface, and look for the Data receive error from Remote Client error message. 2. Ensure that the same encapsulation is configured on the local and the remote multirate interface. 3. Issue the show tsi command on the local and remote equipment. Verify that the Tx time slots of the local interface are the same as the Rx time slots of the remote interface, and vice versa. For more information, refer to the <i>Cisco ONS 15530 Configuration Guide</i>. 4. Ensure that the trunk connection between the 15530 is up.
Error at the remote client.	Issue a show interfaces multirate command to the local multirate interface, and look for the Error at Remote Client error message. The peer client interface is down due one of the following reasons. <ul style="list-style-type: none"> • Administratively down • Down due to Loss of Lock • Down due to Loss of Light • Down due to Loss of Sync

7.3.7 Multirate Interface Detects CVRD Errors

Symptom Multirate interface detects CVRD (code violation and running disparity) errors, and the multirate interface shows Loss of Sync.

Table 7-7 describes the potential causes of the symptom and the solutions.

Table 7-7 *Multirate Interface Detects CVRD Errors*

Possible Problem	Solution
Incorrect protocol encapsulation.	<ol style="list-style-type: none"> 1. Issue a show interfaces command to verify that the correct protocol is configured. 2. If the protocol is incorrect, then issue the encapsulation command to correct the protocol.
Low power level.	Use a power meter to ensure that the receive power level is within the correct range. Adjust the attenuation as needed.
Optical connectors are dirty.	<p>Check the optical connections between the client equipment and the SFP for dirt, bends, or breaks. Clean or replace as necessary.</p> <p>Refer to the <i>Cisco ONS 15530 Cleaning Procedures for Fiber Optic Connections</i> document.</p>

7.3.8 Multirate Interface Not Appearing In Configuration

Symptom A multirate interface does not appear in the configuration.

Table 7-8 describes the potential causes of the symptom and the solutions.

Table 7-8 *Multirate Interface Does Not Appear In Configuration*

Possible Problem	Solution
SFP is not installed.	Inspect the 8-port multi-service muxponder to verify that the SFP is correctly installed.

7.3.9 Encapsulation is Rejected on the Multirate Interface

Symptom A multirate interface does not accept encapsulation.

Table 7-8 describes the potential causes of the symptom and the solutions.

Table 7-9 *Encapsulation is Rejected on the Multirate Interface*

Possible Problem	Solution
Encapsulation type is not supported.	Check the SFP to ensure it supports the required encapsulation.
Invalid rate for the encapsulation.	The SFP IDPROM may be corrupted. Replace the SFP.
TSI channels unavailable.	Issue the show tsi command to confirm that enough STS slots are available to configure the desired protocol.
Old encapsulation still present.	Issue the show interface multirate command to the interface to verify that no encapsulation is configured. If encapsulation is present, issue the no encapsulation command before configuring a new encapsulation.

7.4 Troubleshooting Trunk-Side Interfaces

This section contains troubleshooting procedures for trunk-side interface problems on the 8-port multi-service muxponder.

7.4.1 Wavesonetphy Interface Down and Shows Loss of Lock

Symptom The wavesonetphy interface is down and shows Loss of Lock.

Table 7-10 describes the potential causes of the symptom and the solutions.

Table 7-10 *Wavesonetphy Interface Down and Shows Loss of Lock*

Possible Problem	Solution
Incorrect laser frequency is configured.	Issue the show interfaces wavesonetphy command to verify the configured laser frequency. If necessary, issue the laser frequency command to configure the correct frequency.
The patch cables are incorrectly connected to the OADM module.	Issue the show patch command to verify the patch error status. If it shows a mismatch, connect the wavepatch interface of the 8-port multi-service muxponder to the correct filter ports on the OADM module.
Optical connectors are dirty.	Check the optical connections between the local and remote equipment for dirt, bends, or breaks. Clean or replace as necessary. Refer to the <i>Cisco ONS 15530 Cleaning Procedures for Fiber Optic Connections</i> document.
The patch cables are faulty.	Check the local patch cables between the wavepatch interface of the 8-port multi-service muxponder and the OADM module for bends and breaks. If necessary, replace the patch cable.
Trunk cables are bad.	Check the incoming signal power level. Replace the cables if necessary.
The laser on the remote wavesonetphy interface is shut down.	Issue the no laser shutdown command on the remote wavesonetphy interface.

7.4.2 Wavesonetphy Interface Down and Shows Loss of Frame

Symptom The wavesonetphy interface shows Loss of Frame.

Table 7-11 describes the potential causes of the symptom and the solutions.

Table 7-11 Wavesonetphy Interface Down and Shows Loss of Frame

Possible Problem	Solution
Optical connectors are dirty.	Check the optical connections between the local and remote equipment for dirt, bends, or breaks. Clean or replace as necessary. Refer to the <i>Cisco ONS 15530 Cleaning Procedures for Fiber Optic Connections</i> document.
Excessive attenuation.	Use a power meter to ensure that the receive power level is within specifications for the interface. Reduce the attenuation as needed.
Overload (high receive power).	Use a power meter to ensure that the receive power level is within specifications for the interface. Attenuate the receive path as needed.

7.4.3 B1 Errors on the Wavesonetphy Interface

Symptom The wavesonetphy interface shows B1 errors.

Table 7-12 describes the potential causes of the symptom and the solutions.

Table 7-12 Wavesonetphy Interface Shows B1 Errors

Possible Problem	Solution
The ITU signal power is out of range.	Use a power meter to ensure that the receive power level is within -28 dBm and -8 dBm. Adjust the attenuation as necessary.
Optical connectors are dirty.	Check the optical connections between the local and remote equipment for dirt, bends, or breaks. Clean or replace as necessary. Refer to the <i>Cisco ONS 15530 Cleaning Procedures for Fiber Optic Connections</i> document.

7.4.4 Sdcc Interface Down

Symptom The sdcc interface is down.

Table 7-13 describes the potential causes of the symptom and the solutions.

Table 7-13 Sdcc Interface Down

Possible Problem	Solution
Sdcc interface administratively shut down.	Issue a show interfaces sdcc command to determine the administrative status of the interface. If necessary, issue a no shutdown command to bring it up. Refer to the <i>Cisco ONS 15530 Configuration Guide</i> for more information.
The remote wavesonetphy interface laser is shut down.	Issue the no laser shutdown command on the remote wavesonetphy interface.

7.5 Troubleshooting TSI Protocol Problems

This section contains troubleshooting procedures for time slot interchange (TSI) mapping problems on the 8-port multi-service muxponder. The following example of the **show tsi** command output displays the TSI mapping of the Cisco ONS 15530 system:

Local system.

```
Switch1_1#show tsi
Port   Local   Peer   Error   Trunk STS Map
      Encap Encap   Transmit Receive

Card:9, TSI Ver:1, DCC:SDCC9/0/0, TSI-Protocol:Enabled

 0.  T1     T1     -       00 00 00 00 00 01   00 00 00 00 00 01
 1.  FC1    FC1    -       00 FF FE 00 00 0E   00 00 00 07 FF FE
 2.  T1     T1     -       00 00 00 00 00 01   00 00 00 00 00 01
 3.  CFE    CFE    -       07 00 00 00 00 00   00 00 00 38 00 00
 4.  E1     E1     -       00 00 00 00 00 01   00 00 00 00 00 01
 5.  CGE    CGE    -       00 00 01 FF FF F0   07 FF FF C0 00 00
 6.  T1     ESCON  M       00 00 00 00 00 01   78 00 00 00 00 00
 7.  None   None   -


Available STS= 5
-----
```

7.5.1 End-to-End Traffic Not Flowing Due to TSI Problems

Symptom End-to-end traffic is not flowing due to TSI problems.

Table 7-14 describes the potential causes of the symptom and the solutions.

Table 7-14 *End-to-End Traffic Not Flowing Due to TSI Problems*

Possible Problem	Solution
After configuring the encapsulation on the multirate interface a TSI mismatch alarm is seen on the console.	<ol style="list-style-type: none"> 1. Issue the show tsi command to verify that both the local and remote equipment encapsulation are configured correctly. Both ends must be the same. An M in the error column of the output indicates an encapsulation mismatch between the local and remote ends. 2. If the local and remote Rx and Tx STS maps do not match, remove the encapsulation on the local multirate interface with the no encapsulation command and then reconfigure the encapsulation with the encapsulation command.
	 <p>Note To change the interface encapsulation you must first shut down the multirate interface.</p>
The show tsi command output does not display the Rx STS maps.	<ol style="list-style-type: none"> 1. Confirm the sdcc interface is up and OSCP is in a 2-way state on both the local and remote switches. 2. Make sure TSI is enabled on both the local and remote switches

7.6 Troubleshooting 8-Port Multi-Service Muxponder Problems Using Loopbacks

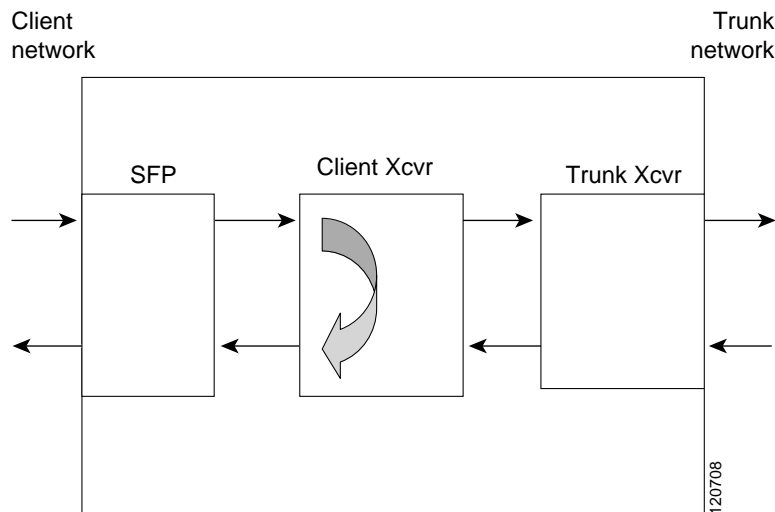
This section describes how to use software loopbacks to perform fault isolation for signals on 8-port multi-service muxponders. The 8-port multi-service muxponder supports two types of software loopbacks on the client-side and trunk-side interfaces:

- Facility loopbacks
- Terminal loopbacks

7.6.1 Client-Side Facility Loopbacks

Client-side facility loopbacks on 8-port multi-service muxponders verify the functioning of the SFP optics from the client side (see Figure 7-2).

Figure 7-2 Client-Side Facility Loopback Example



Note

For T1 and E1 encapsulations the loopback is performed on the SFP, not the client Xcvr.

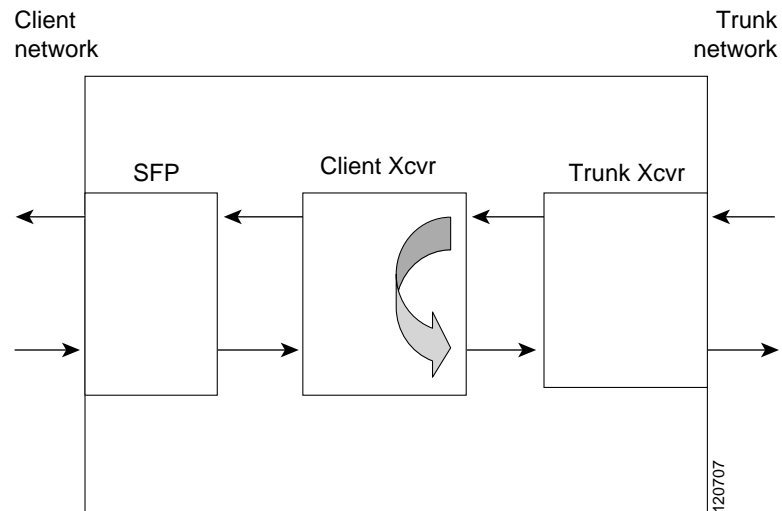
To create a client-side facility loopback:

- Step 1** Issue a **loopback facility** command on the multirate interface.
- Step 2** Check that the traffic is reaching the client equipment.
- Step 3** If the signal does not reach the client equipment, replace the SFP optics.

7.6.2 Client-Side Terminal Loopbacks

Client-side terminal loopbacks verify the functioning of the 8-port multi-service muxponders from the trunk side (see Figure 7-3).

Figure 7-3 Client-Side Terminal Loopback Example



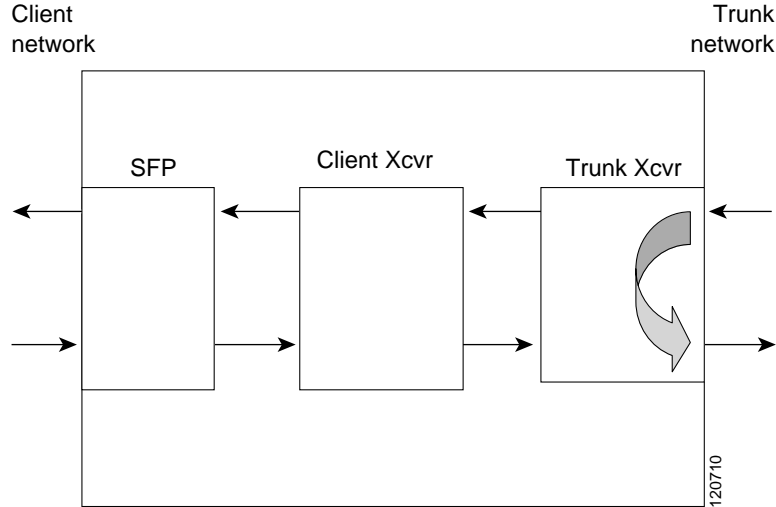
Note For T1 and E1 encapsulations the loopback is performed on the SFP, not the client Xcvr.

To create a client-side terminal loopback:

- Step 1** Issue a **loopback terminal** command on the multirate interface.
- Step 2** Check that the traffic is reaching the remote client equipment.
- Step 3** If the signal does not reach the far end, check the trunk fiber and the interfaces along the signal path. If the fiber is intact, replace the 8-port multi-service muxponder.

7.6.3 Trunk-Side Facility Loopbacks

Trunk-side facility loopbacks on the wavesonetphy interface of the 8-port multi-service muxponders verify the functioning of the trunk optics from the trunk side (see Figure 7-4).

Figure 7-4 Trunk-Side Facility Loopback Example

To create a trunk-side facility loopback:

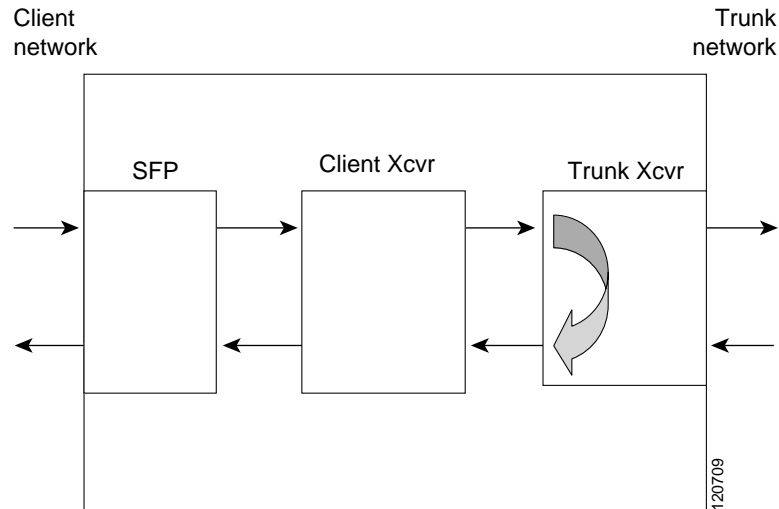
-
- Step 1** Issue a **loopback facility** command on the wavesonetphy interface.
 - Step 2** Check that the traffic is reaching the remote client equipment.
 - Step 3** If the signal does not reach the far end, check the trunk fiber and the interfaces along the signal path. If the fiber is intact, replace the 8-port multi-service muxponder.
-

7.6.4 Trunk-Side Terminal Loopbacks

Trunk-side terminal loopbacks verify the functioning of the 8-port multi-service muxponders from the client side, up to the trunk side (see Figure 7-5).



Note Trunk side optics are not tested.

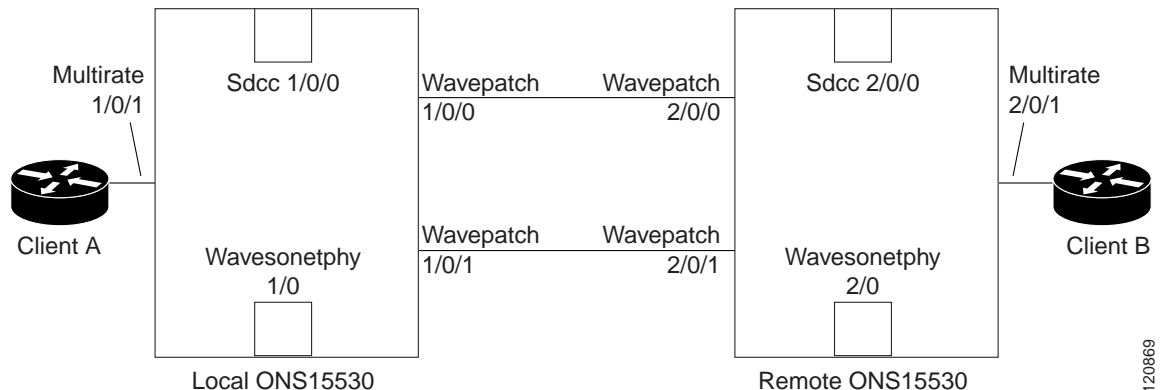
Figure 7-5 Trunk-Side Terminal Loopback Example

To create a trunk-side terminal loopback:

-
- Step 1** Issue a **loopback terminal** command on the wavesonetphy interface.
 - Step 2** Check that the traffic is reaching the client equipment.
 - Step 3** If the signal does not reach the client equipment check the cables for bends and breaks, and if necessary, replace the SFP optics.
-

7.6.5 Troubleshooting Protocol Level Errors in an End-to-End Scenario

Figure 7-6 shows an example of 8-port multi-serve muxponders connected end-to-end. The following procedure describes the process of troubleshooting protocol level errors (for example, CRC errors on a Fastethernet interface) using loopbacks. Assume that the trunk connection between wavepatch 1/0/0 and wavepatch 2/0/0 is active.

Figure 7-6 8-Port Multi-Service Muxponders in an End-to-End Configuration

-
- Step 1** Issue a **loopback facility** command on multirate interface 1/0/1 of client A. Verify that traffic comes back to client A without errors. If errors are seen, one of the following may be the cause:
- Client A itself is sending traffic with errors.
 - The optical connectors between client A and the local Cisco ONS 15530 are dirty or need to be replaced.
 - The SFP on the multirate interface is faulty.
- If no errors occur, proceed to Step 2.
- Step 2** Issue a **no loopback facility** command on multirate interface 1/0/1 of the local Cisco ONS 15530, and issue a **loopback terminal** command on wavesonetphy 1/0 of the local Cisco ONS 15530. If errors occur, replace the 8-port multi-service muxponder. If no errors occur, proceed to Step 3.
- Step 3** Issue a **no loopback terminal** command on wavesonetphy 1/0 of the local Cisco ONS 15530 and issue a **loopback facility** command on wavesonetphy 2/0 on the remote Cisco ONS 15530. If errors are seen on client A, one of the following may be the cause:
- The optical connectors between the local Cisco ONS 15530 and the remote Cisco ONS 15530 are dirty or need to be replaced.
 - The 8-port multi-service muxponder on the remote Cisco ONS 15530 is faulty.
- If no errors occur, proceed to Step 4.
- Step 4** Issue a **no loopback facility** command on wavesonetphy 2/0 of the remote Cisco ONS 15530, and issue a **loopback terminal** command on multirate 2/0/1 on the remote Cisco ONS 15530. If errors are seen on client A, replace the 8-port multi-service muxponder in the remote Cisco ONS 15530. If no errors occur, proceed to Step 5.
- Step 5** Issue a **loopback facility** command on multirate 2/0/1 of the remote Cisco ONS 15530. If errors are seen at client B the optical connectors between client B and the remote Cisco ONS 15530 are dirty or need to be replaced.

**Note**

This procedure can also be used to troubleshoot traffic not flowing in an end-to-end scenario.



Troubleshooting 2.5-Gbps ITU Trunk Card Problems

This chapter describes how to troubleshoot 2.5-Gbps ITU trunk card problems. This chapter includes the following sections:

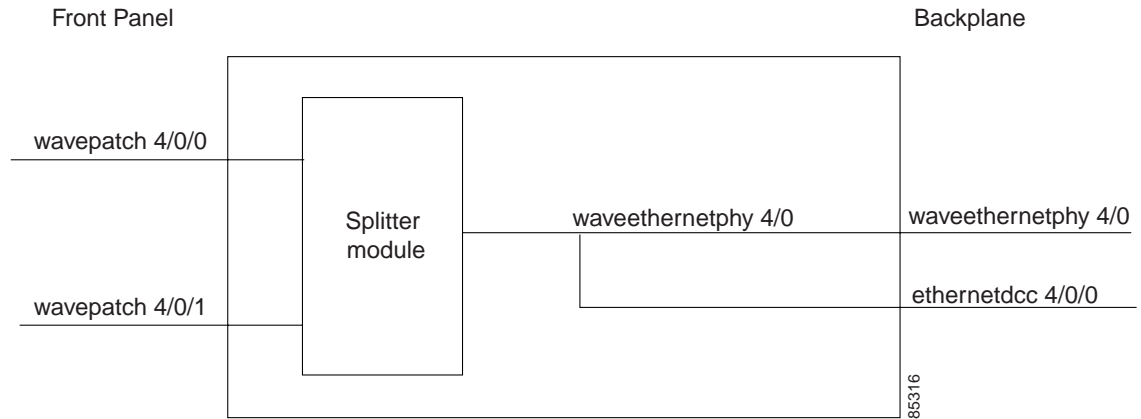
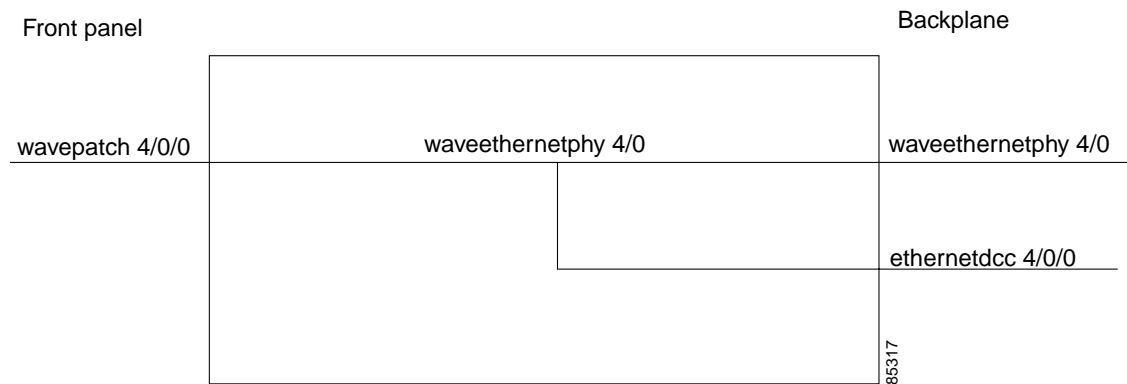
- 8.1 Overview, page 8-1
- 8.2 Initial Troubleshooting Checklist, page 8-2
- 8.3 Troubleshooting 2.5-Gbps ITU Trunk Card Interface Problems, page 8-3
- 8.4 Troubleshooting 2.5-Gbps ITU Trunk Card Problems Using Loopbacks, page 8-5

8.1 Overview

The 2.5-Gbps ITU trunk card converts an aggregated 2.5-Gbps signal to an ITU-compliant wavelength, or channel. The Cisco ONS 15530 supports two types of 2.5-Gbps ITU trunk cards:

- Splitter—Sends the channels to two OADM modules.
- Nonsplitter—Sends the channel to only one OADM module.

Figure 8-1 and Figure 8-2 show the interface models for the two versions of the 2.5-Gbps ITU trunk card, splitter and nonsplitter.

Figure 8-1 Splitter 2.5-Gbps ITU Trunk Card Interfaces**Figure 8-2** Nonsplitter 2.5-Gbps ITU Trunk Card Interfaces

8.2 Initial Troubleshooting Checklist

Follow this initial checklist before proceeding with the troubleshooting procedures:

- Check that the receive signal power level is between -28 dBm and -8 dBm.
- Issue **show interfaces** commands to ensure that the waveethernetphy and wavepatch interfaces are administratively up, that there are no errors on the interfaces, and that the laser frequency is correctly configured.
- Issue a **show connect** command to verify the status of the cross connections to the aggregation card.
- Check that the LEDs on the cards show the proper state.
- Issue a **show facility-alarm status** command to display the alarms on the interfaces.

- Issue the **show hardware linecard** command to verify the 2.5-Gbps ITU trunk card functional image.
- Check that the 2.5-Gbps ITU trunk cards are patched to the correct OADM ports. Issue a **show patch** command to verify that there are no frequency mismatches.
- Ensure that all optical connectors are clean. Refer to the *Cisco ONS 15530 Cleaning Procedures for Fiber Optic Connections* document.

8.3 Troubleshooting 2.5-Gbps ITU Trunk Card Interface Problems

This section contains troubleshooting procedures for 2.5-Gbps ITU trunk card interface problems.

8.3.1 Waveethernetphy Interface Down and Shows Loss of Lock

Symptom The waveethernetphy interface is in a down state and the signal quality shows a Loss of Lock. Table 8-1 describes the potential causes of the symptom and the solutions.

Table 8-1 Waveethernetphy Interface Down and Shows Loss of Lock

Possible Problem	Solution
The laser frequency is not correctly configured.	Check the configured laser frequency in the show interfaces waveethernetphy command output. If it is incorrect, issue the laser frequency command to configure the correct frequency.
The patch cables are incorrectly connected to the OADM module.	Check the patch error status in the show patch command output. If it shows a mismatch, connect the 2.5-Gbps ITU trunk card to the correct filter ports on the OADM module.
The optical connectors are dirty.	Refer to the <i>Cisco ONS 15530 Cleaning Procedures for Fiber Optic Connections</i> document.
The protocol traffic is incorrect.	Compare the remote traffic source on the channel with the local destination. If the cards or protocol encapsulations are different, correct the problem.
The patch cables are faulty.	Check the local patch cables between the 2.5-Gbps ITU trunk card and the OADM module for breaks. If there is a break, replace the patch cable.
The trunk cables are broken.	Check the incoming signal power level. Fix any problems with the fiber.

8.3.2 Waveethernetphy Interface Down and Shows Loss of Sync

Symptom The waveethernetphy interface is in a down state and the signal quality shows a Loss of Sync. Also, the **show facility-alarm status** command output shows an alarm message.

Table 8-2 describes the potential causes of the symptom and the solutions.

Table 8-2 Waveethernetphy Interface Down and Shows Loss of Sync

Possible Problem	Solution
The ITU signal power is too high or too low.	Check the signal power from the OADM module. Ensure that it is between –28 dBm and –8 dBm. If not, adjust the attenuation.
The remote client interface reported errors.	Verify that the client interface on the remote system is not reporting errors. Resolve any error conditions.
An interface in the signal path has errors.	Issue the show interfaces commands for the interfaces in the signal path to determine if errors are occurring.
The optical connectors are dirty.	Refer to the <i>Cisco ONS 15530 Cleaning Procedures for Fiber Optic Connections</i> document.
The patch cables are faulty.	Check the local patch cables between the 2.5-Gbps ITU trunk card and the OADM module for breaks. If there is a break, replace the patch cable.
The trunk cables are faulty.	Check the incoming signal power level. Fix any problems with the fiber.

8.3.3 CVRD Errors on the Waveethernetphy Interface

Symptom The waveethernetphy interface is in a down state and in the **show interfaces** command output the Code violation and running disparity error count (64b66b CVRD) field are increasing and the Signal Condition field shows “Signal Fail Threshold exceeded.”

Table 8-3 describes the potential causes of the symptom and the solutions.

Table 8-3 CVRD Errors on the Waveethernetphy Interface

Possible Problem	Solution
The ITU signal power is too high or too low.	Check the signal power from the OADM module. Ensure that it is between –28 dBm and –8 dBm. If not, adjust the attenuation.
The optical connectors are dirty.	Refer to the <i>Cisco ONS 15530 Cleaning Procedures for Fiber Optic Connections</i> document.
The patch cables are faulty.	Check the local patch cables between the 2.5-Gbps ITU trunk card and the OADM module for pinches or breaks. Correct any problems with the fiber.
The trunk cables are faulty.	Check the trunk fiber for pinches or breaks. Correct any problems with the fiber.

8.3.4 CRC and CDL HEC Errors on the Waveethernetphy Interface

Symptom The waveethernetphy interface is in a down state, the CRC error count and the CDL HEC error counts in the **show interfaces** command output is increasing, and the Signal Condition field shows “Signal Fail Threshold exceeded” or “Signal Degrade Threshold exceeded.”

Table 8-3 describes the potential causes of the symptom and the solutions.

Table 8-4 CRC and CDL HEC Errors on the Waveethernetphy Interface

Possible Problem	Solution
The data is corrupted somewhere in the data path.	<ol style="list-style-type: none"> 1. Perform a loopback on the signal path to isolate the area where the data is corrupted. For information on performing loopbacks, see the “8.4 Troubleshooting 2.5-Gbps ITU Trunk Card Problems Using Loopbacks” section on page 8-5. 2. Issue show interfaces commands for all the interfaces in the signal path. Resolve any error conditions or configuration problems encountered.

8.3.5 Ethernetdcc Interface Down

Symptom The ethernetdcc interface is down and pings across the interface fail.

Table 8-5 describes the potential cause of the symptom and the solution.

Table 8-5 Ethernetdcc Interface Down

Possible Problem	Solution
The ethernetdcc interface is administratively shut down.	<ol style="list-style-type: none"> 1. Issue a show interfaces command to determine the administrative status of the ethernetdcc interface. 2. Issue a no shutdown command to bring it up, if necessary.

8.4 Troubleshooting 2.5-Gbps ITU Trunk Card Problems Using Loopbacks

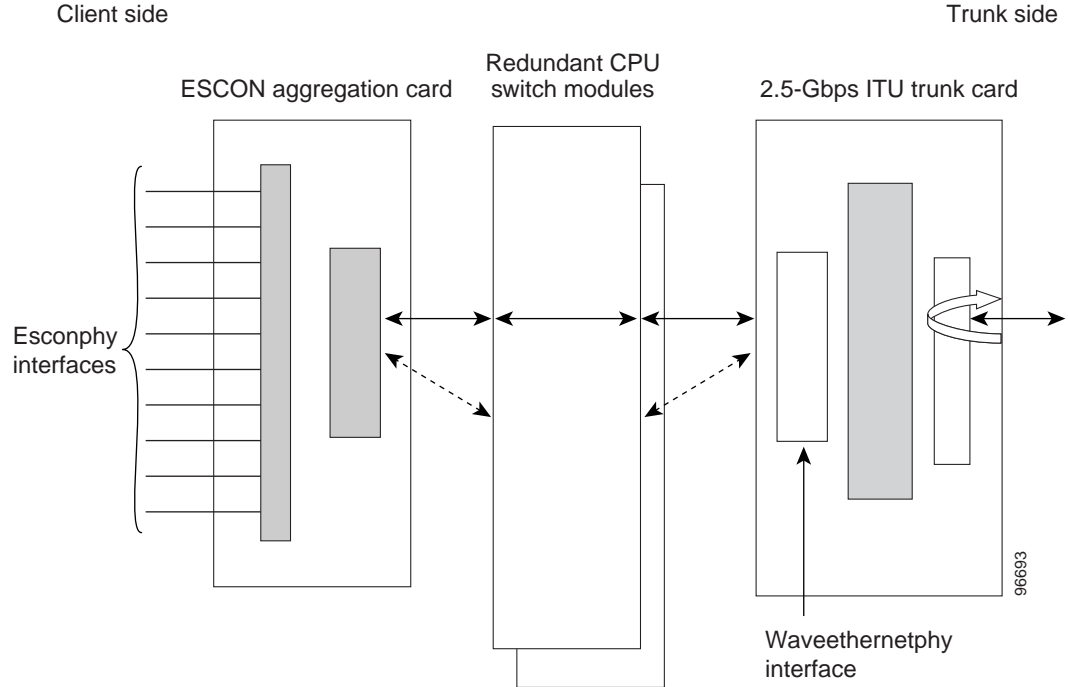
This section describes how to use software loopbacks to perform fault isolation for signals on 2.5-Gbps ITU trunk cards. The 2.5-Gbps ITU trunk card supports two types of software loopbacks:

- Facility loopbacks
- Terminal loopbacks

8.4.1 Facility Loopbacks

A facility loopback verifies the functioning of the 2.5-Gbps ITU trunk card from the trunk side (see Figure 8-3).

Figure 8-3 Facility Loopback Example on a 2.5-Gbps ITU Trunk Card

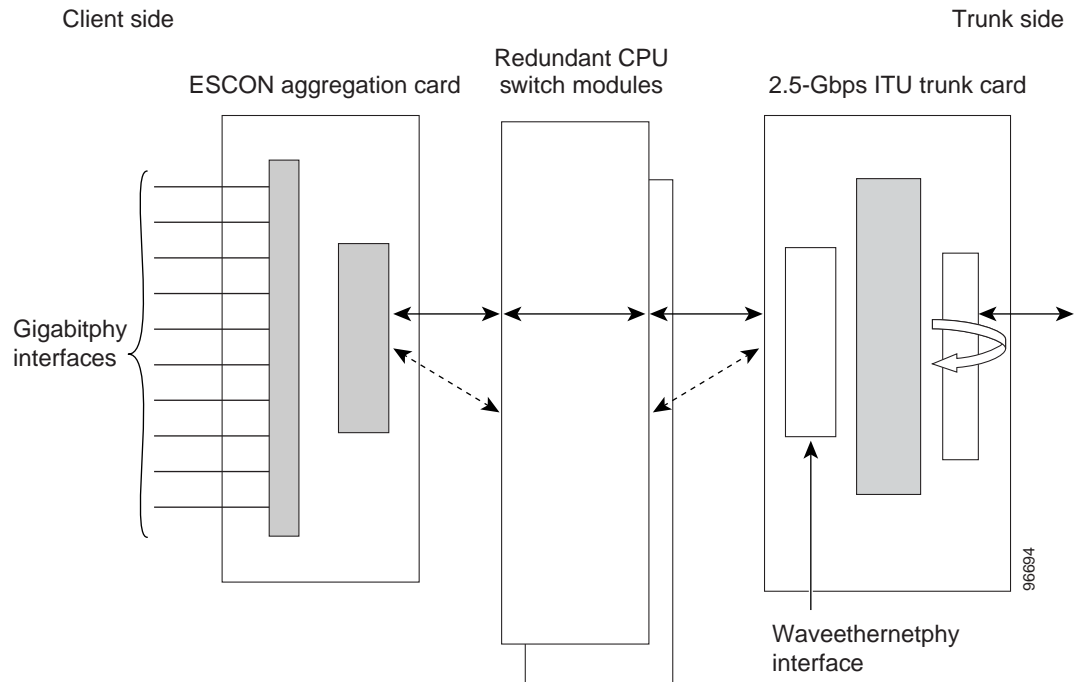


Procedure: Create a Facility Loopback

-
- Step 1** Issue a **loopback facility** command on the waveethernetphy interface.
 - Step 2** Check that the signal reaches the system at the far end.
 - Step 3** If the signal does not reach the far end, check the trunk fiber and the interfaces along the signal path. If the fiber is intact, replace the card.
-

8.4.2 Terminal Loopbacks

A terminal loopback verifies the functioning of the 2.5-Gbps ITU trunk card from the switch fabric side (see Figure 8-4).

Figure 8-4 Terminal Loopback Example on a 2.5-Gbps ITU Trunk Card

To create a terminal loopback:

-
- Step 1** Issue a **loopback terminal** command on the waveethernetphy interface.
 - Step 2** Check that the traffic is reaching the client equipment.
 - Step 3** If the signal does not reach the client equipment, replace the card.
-



Troubleshooting 10-Gbps ITU Trunk Card Problems

This chapter describes how to troubleshoot 10-Gbps ITU trunk card problems. This chapter includes the following sections:

- 9.1 Overview, page 9-1
- 9.2 Initial Troubleshooting Checklist, page 9-3
- 9.3 Troubleshooting 10-Gbps ITU Trunk Card Interface Problems, page 9-3
- 9.4 Troubleshooting 10-Gbps ITU Trunk Card Problems Using Loopbacks, page 9-5

9.1 Overview

The 10-Gbps ITU trunk card converts up to four aggregated signals to an ITU-compliant wavelength, or channel.

Figure 9-1 shows the interfaces for the splitter 10-Gbps ITU trunk card. Figure 9-2 shows the interfaces for the nonsplitter 10-Gbps ITU trunk card.

Figure 9-1 Splitter 10-Gbps ITU Trunk Card Interfaces

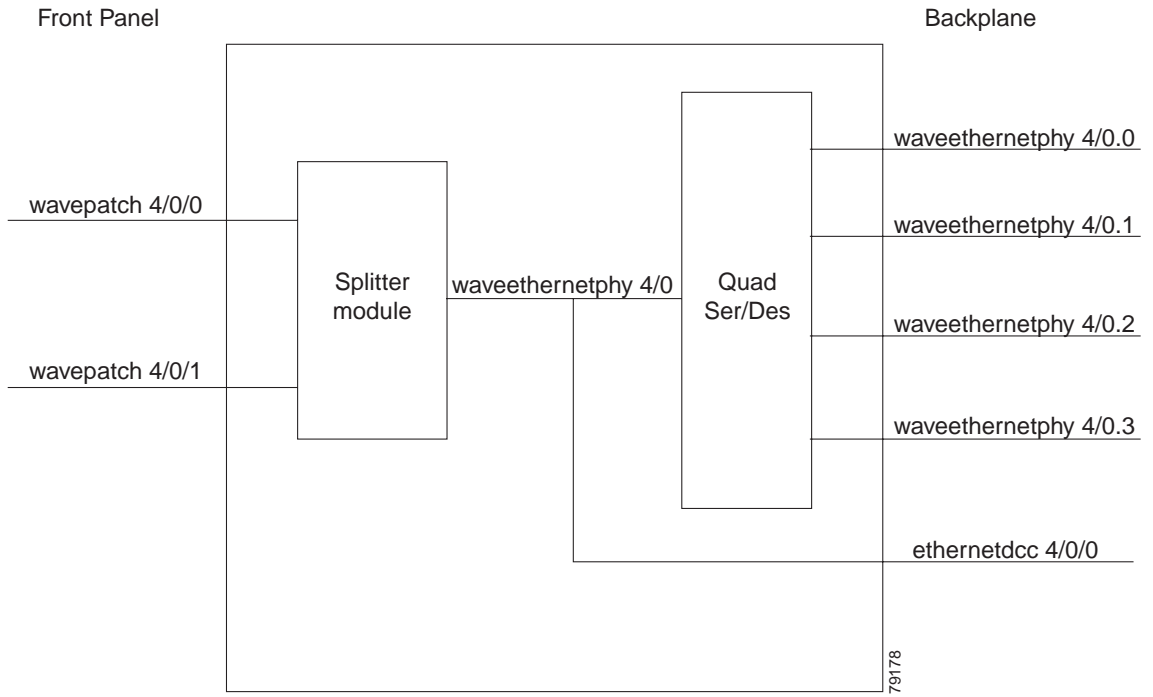
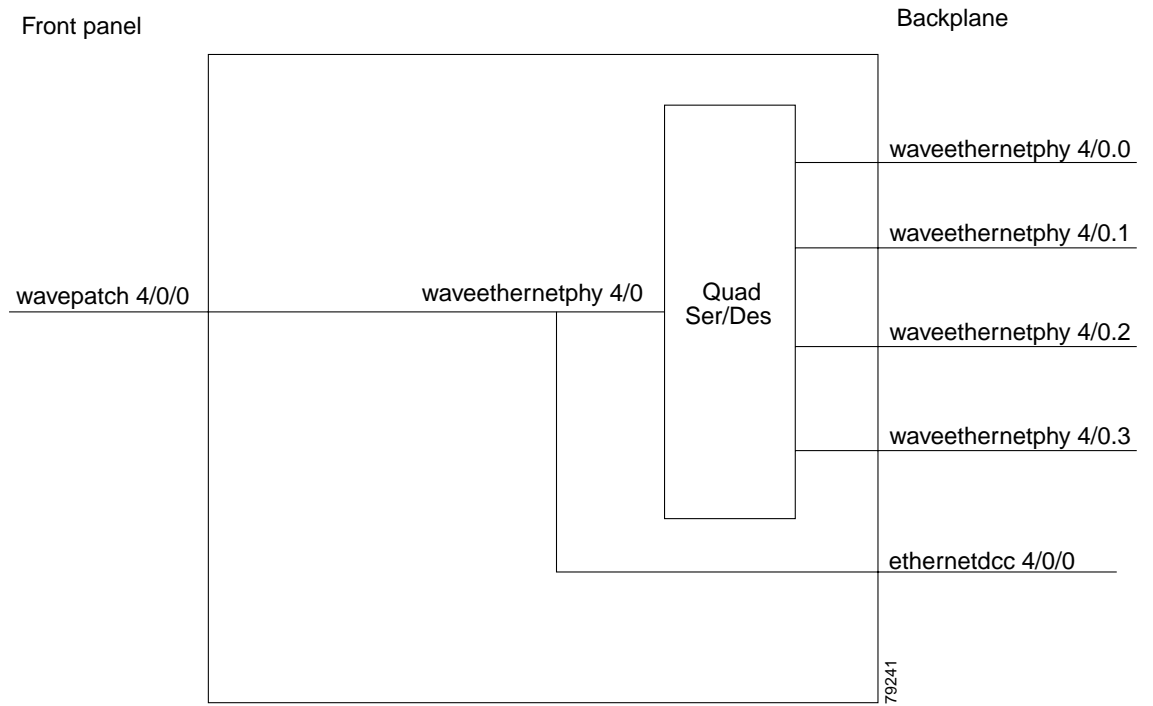


Figure 9-2 Nonsplitter 10-Gbps ITU Trunk Card Interfaces



9.2 Initial Troubleshooting Checklist

Follow this initial checklist before proceeding with the troubleshooting procedures:

- Check that the receive signal power level is between -22 dBm and -6 dBm.
- Issue **show interfaces** commands to ensure that the waveethernetphy and wavepatch interfaces are administratively up, that there are no errors on the interfaces, and that the ITU laser is up.
- Issue a **show connect** command to verify the status of the cross connections to the aggregation cards.
- Check that the LEDs on the cards show the proper state.
- Issue a **show facility-alarm status** command to display the alarms on the interfaces.
- Issue the **show hardware linecard** command to verify the 10-Gbps ITU trunk card functional image.
- Check that the 10-Gbps ITU trunk cards are patched to the correct OADM ports. Issue a **show patch** command to verify that there are no frequency mismatches.
- Ensure that all optical connectors are clean. Refer to the *Cisco ONS 15530 Cleaning Procedures for Fiber Optic Connections* document.

9.3 Troubleshooting 10-Gbps ITU Trunk Card Interface Problems

This section contains troubleshooting procedures for 10-Gbps ITU trunk card interface problems.

9.3.1 Waveethernetphy Interface Down and Shows Loss of Lock

Symptom A waveethernetphy interface is down and signal quality status shows Loss of Lock.

Table 9-1 describes the potential causes of the symptom and the solutions.

Table 9-1 Waveethernetphy Interface Down and Shows Loss of Lock

Possible Problem	Solution
The patch cables are incorrectly connected to the OADM module.	Check the patch error status in the show patch command output. If it shows a mismatch, correct the patch the 10-Gbps ITU trunk card to the correct filter ports on the OADM module.
The laser frequency is not correctly configured.	Check the configured laser frequency in the show interfaces waveethernetphy command output. If it is incorrect, issue the laser frequency command to configure the correct frequency.
The optical connectors are dirty.	Refer to the <i>Cisco ONS 15530 Cleaning Procedures for Fiber Optic Connections</i> document.
The ITU signal power is too low or too high.	Check the signal power received from the OADM module. Ensure that it is between -22 dBm and -6 dBm. If not, adjust the attenuation.
The trunk fiber is broken.	Check the signal power received from the trunk. If below -22 dBm, check for trunk fiber breaks.

9.3.2 Waveethernetphy Interface Down and Shows Loss of Sync

Symptom A waveethernetphy interface is down and signal quality status shows Loss of Sync.

Table 9-1 describes the potential causes of the symptom and the solution.

Table 9-2 Waveethernetphy Interface Down and Shows Loss of Sync

Possible Problem	Solution
The optical connectors are dirty.	Refer to the <i>Cisco ONS 15530 Cleaning Procedures for Fiber Optic Connections</i> document.
The ITU signal power is too low.	Check the signal power received from the OADM module. Ensure that it is between -22 dBm and -6 dBm. If not, adjust the attenuation.
The remote client interface reported errors.	Verify that the client interface on the remote system do not report errors. Resolve any error conditions.
An interface in the signal path has errors.	Issue the show interfaces commands for the interfaces in the signal path to determine if errors occur.
The trunk fiber is broken.	Check the signal power received from the trunk. If below -22 dBm, check for trunk fiber breaks.

9.3.3 CVRD Errors on the Waveethernetphy Interface

Symptom The waveethernetphy interface is in a down state and in the **show interfaces** command output the Code violation and running disparity error count (64b66b CVRD) field are increasing and the Signal Condition field shows “Signal Fail Threshold exceeded.”

Table 9-3 describes the potential causes of the symptom and the solutions.

Table 9-3 CVRD Errors on the Waveethernetphy Interface

Possible Problem	Solution
The ITU signal power is too high or too low.	Check the signal power from the OADM module. Ensure that it is between -22 dBm and -6 dBm. If not, adjust the attenuation.
The optical connectors are dirty.	Refer to the <i>Cisco ONS 15530 Cleaning Procedures for Fiber Optic Connections</i> document.
The trunk cables are faulty.	Check the trunk fiber for pinches or breaks. Correct any problems with the fiber.
The patch cables are faulty.	Check the local patch cables between the 10-Gbps ITU trunk card and the OADM module for pinches or breaks. Correct any problems with the fiber.

9.3.4 CRC and CDL HEC Errors on the Waveethernetphy Interface

Symptom The waveethernetphy interface is in a down state, the CRC error count and the CDL HEC error counts in the **show interfaces** command output is increasing, and the Signal Condition field shows “Signal Fail Threshold exceeded” or “Signal Degrade Threshold exceeded.”

Table 9-4 describes the potential causes of the symptom and the solutions.

Table 9-4 CRC and CDL HEC Errors on the Waveethernetphy Interface

Possible Problem	Solution
The data is corrupted somewhere in the data path.	<ol style="list-style-type: none"> 1. Perform a loopback on the signal path to isolate the area where the data is corrupted. For information on performing loopbacks, see the “9.4 Troubleshooting 10-Gbps ITU Trunk Card Problems Using Loopbacks” section on page 9-5. 2. Issue show interfaces commands for all the interfaces in the signal path. Resolve any error conditions or configuration problems encountered.

9.3.5 Ethernetdcc Interface Down

Symptom The ethernetdcc interface is down and pings across the interface fail.

Table 9-5 describes the potential cause of the symptom and the solution.

Table 9-5 Ethernetdcc Interface Down

Possible Problem	Solution
The ethernetdcc interface is administratively shut down.	Issue the show interfaces command to determine the administrative status of the ethernetdcc interface. If it is administratively shut down, issue the no shutdown command to bring it up.

9.4 Troubleshooting 10-Gbps ITU Trunk Card Problems Using Loopbacks

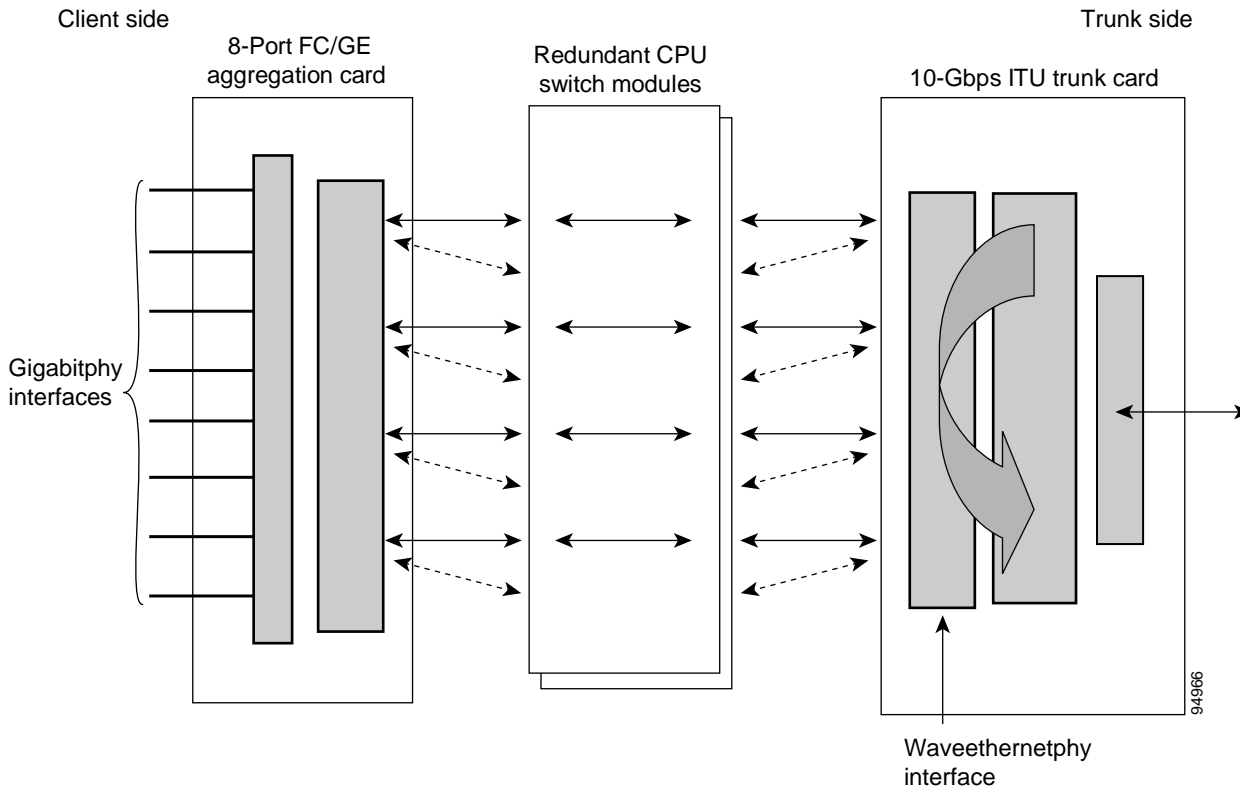
This section describes how to use software loopbacks to perform fault isolation for signals on 10-Gbps ITU trunk cards. The 10-Gbps ITU trunk card supports two types of software loopbacks:

- Facility loopbacks
- Terminal loopbacks

9.4.1 Facility Loopbacks

A facility loopback verifies the functioning of the 10-Gbps ITU trunk card from the trunk side (see Figure 9-3).

Figure 9-3 Facility Loopback Example on a 10-Gbps ITU Trunk Card



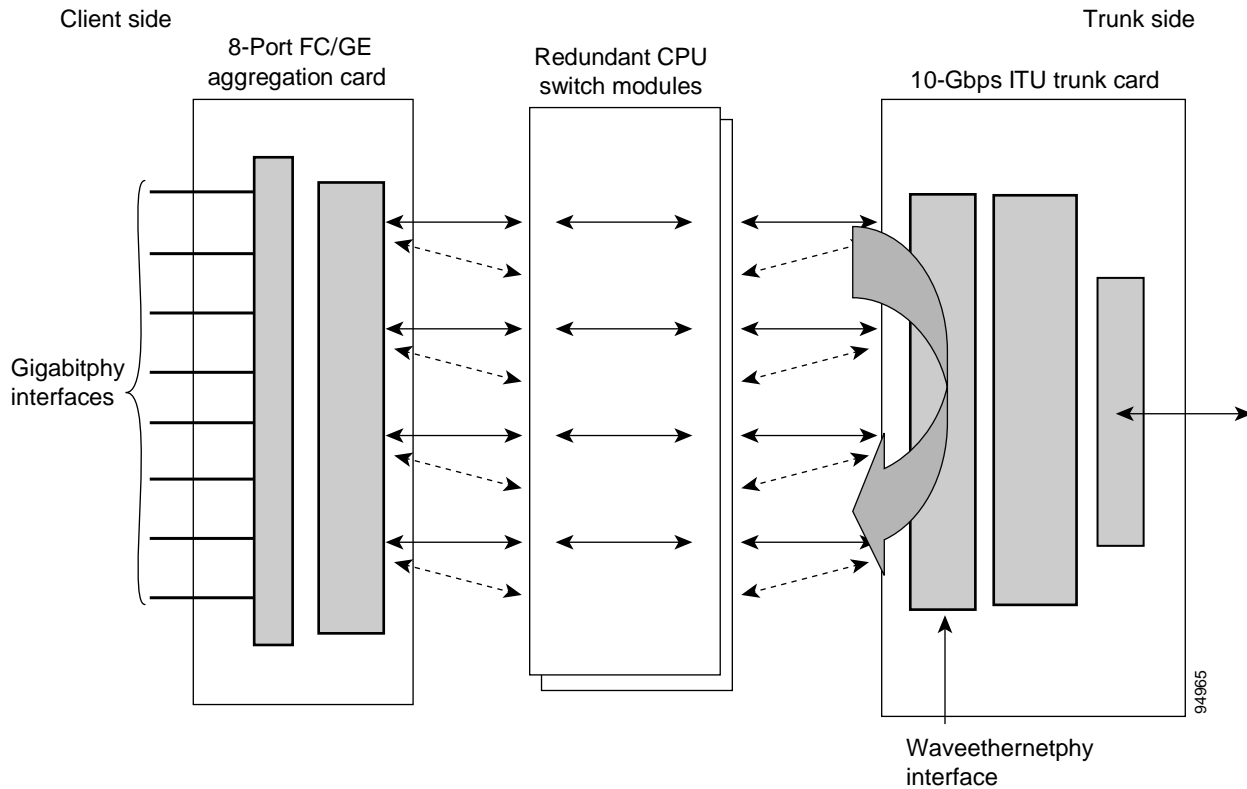
To create a facility loopback

-
- Step 1** Issue a **loopback facility** command on the waveethernetphy interface.
 - Step 2** Check that the signal reaches the system at the far end.
 - Step 3** If the signal does not reach the far end, check the trunk fiber and the interfaces along the signal path. If the fiber is intact, replace the card.
-

9.4.2 Terminal Loopbacks

A terminal loopback verifies the functioning of the 10-Gbps ITU trunk card from the switch fabric side (see Figure 9-4).

Figure 9-4 Terminal Loopback Example on a 10-Gbps ITU Trunk Card



To create a terminal loopback:

-
- Step 1** Issue a **loopback terminal** command on the waveethernetphy interface.
 - Step 2** Check that the traffic is reaching the client equipment.
 - Step 3** If the signal does not reach the client equipment, replace the card.
-



Troubleshooting 10-Gbps ITU Tunable Trunk Card Problems

This chapter describes how to troubleshoot 10-Gbps ITU tunable trunk card problems. This chapter includes the following sections:

- 10.1 Overview, page 10-1
- 10.2 Initial Troubleshooting Checklist, page 10-3
- 10.3 Troubleshooting 10-Gbps ITU Tunable Trunk Card Interface Problems, page 10-3
- 10.4 Troubleshooting 10-Gbps ITU Tunable Trunk Card Problems Using Loopbacks, page 10-6

10.1 Overview

The 10-Gbps ITU tunable trunk card converts up to four aggregated signals to an ITU-compliant wavelength, or channel.

Figure 10-1 shows the interfaces for the splitter 10-Gbps ITU tunable trunk card. Figure 10-2 shows the interfaces for the nonsplitter 10-Gbps ITU tunable trunk card.

Figure 10-1 Splitter 10-Gbps ITU Tunable Trunk Card Interfaces

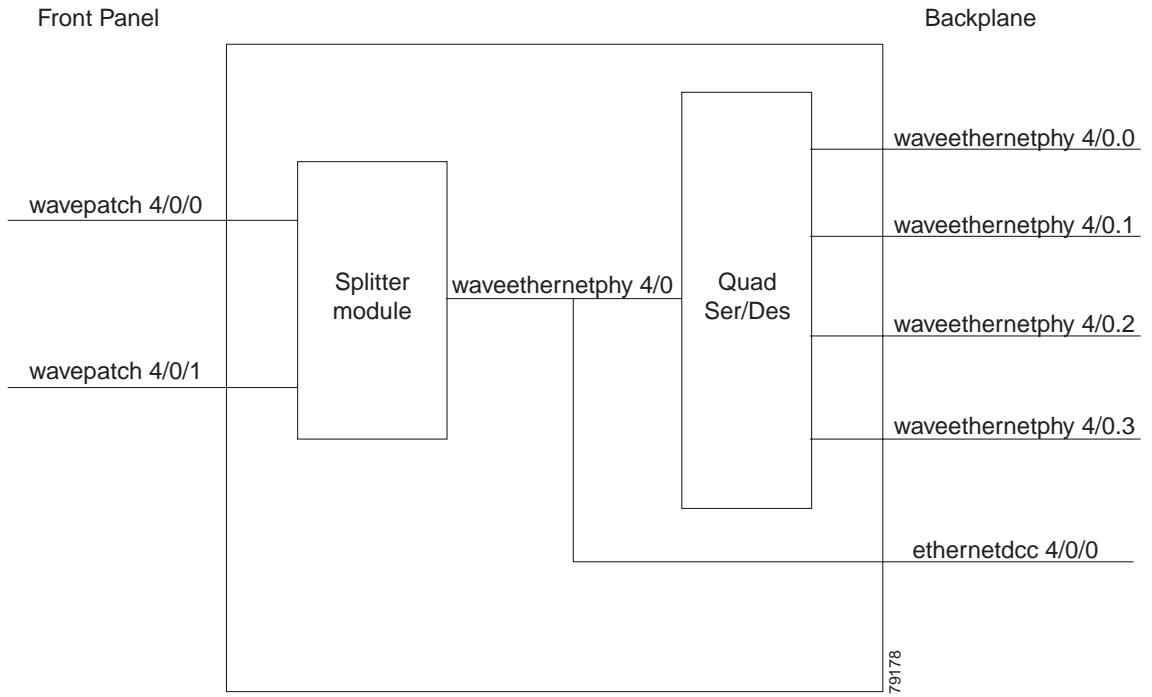
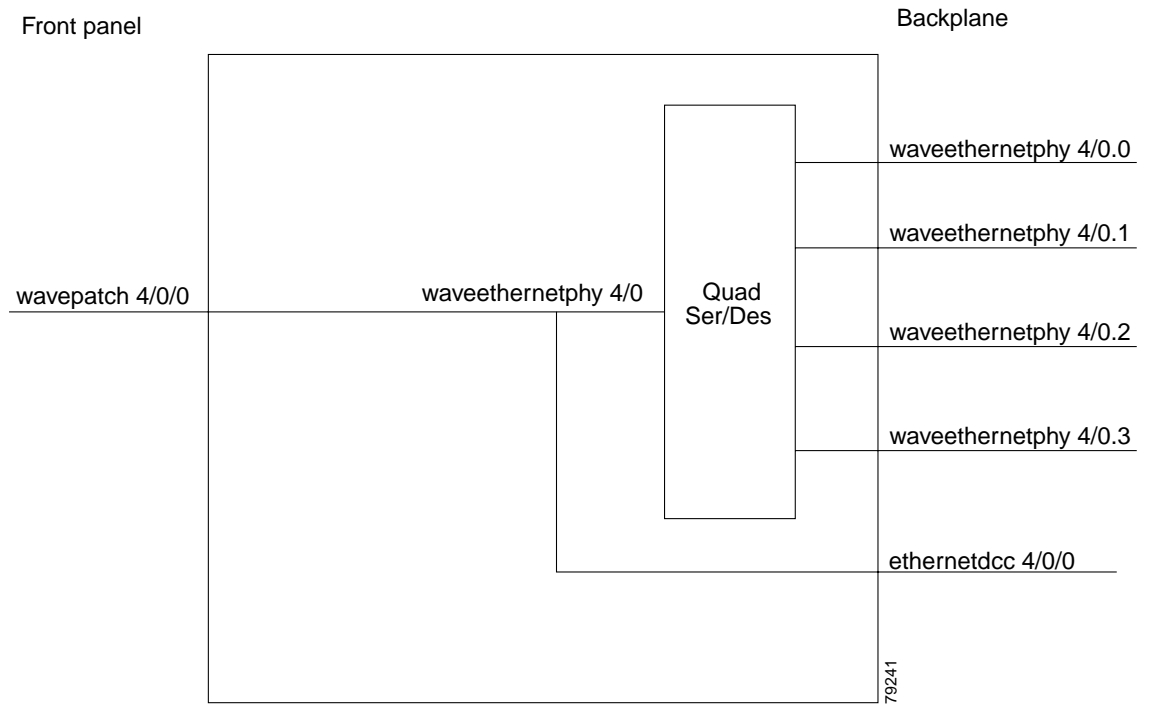


Figure 10-2 Nonsplitter 10-Gbps ITU Tunable Trunk Card Interfaces



10.2 Initial Troubleshooting Checklist

Follow this initial checklist before proceeding with the troubleshooting procedures:

- Check that the receive signal power level is between -22 dBm and -6 dBm.
- Issue **show interfaces** commands to ensure that the waveethernetphy and wavepatch interfaces are administratively up, that there are no errors on the interfaces, and that the ITU laser is up.
- Issue a **show connect** command to verify the status of the cross connections to the aggregation cards.
- Check that the LEDs on the cards show the proper state.
- Issue a **show facility-alarm status** command to display the alarms on the interfaces.
- Issue the **show hardware linecard** command to verify the 10-Gbps ITU tunable trunk card functional image.
- Issue **show interfaces** command and make sure that the correct frequency is configured on the waveethernetphy interface of 10-Gig ITU tunable trunk card.
- Check that the 10-Gbps ITU tunable trunk cards are patched to the correct OADM ports according to the configured frequency. Issue a **show patch** command to verify that there are no frequency mismatches.
- Ensure that all optical connectors are clean. Refer to the *Cisco ONS 15530 Cleaning Procedures for Fiber Optic Connections* document.

10.3 Troubleshooting 10-Gbps ITU Tunable Trunk Card Interface Problems

This section contains troubleshooting procedures for 10-Gbps ITU tunable trunk card interface problems.

10.3.1 Waveethernetphy Interface Down and Shows Loss of Lock

Symptom A waveethernetphy interface is down and signal quality status shows Loss of Lock.

Table 10-1 describes the potential causes of the symptom and the solutions.

Table 10-1 Waveethernetphy Interface Down and Shows Loss of Lock

Possible Problem	Solution
The laser frequency is not correctly configured.	Check the configured laser frequency in the show interfaces waveethernetphy command output. If it is incorrect, issue the laser frequency command to configure the correct frequency.
The patch cables are incorrectly connected to the OADM module.	Check whether patch cables are connected according to the configured frequency of 10-Gbps ITU tunable trunk card. Also, check the patch error status in the show patch command output. If it shows a mismatch, correct the patch of the 10-Gbps ITU tunable trunk card to the correct filter ports on the OADM module.

Table 10-1 Waveethernetphy Interface Down and Shows Loss of Lock

Possible Problem	Solution
The laser frequency is not correctly configured.	Check the configured laser frequency in the show interfaces waveethernetphy command output. If it is incorrect, issue the laser frequency command to configure the correct frequency.
The optical connectors are dirty.	Refer to the <i>Cisco ONS 15530 Cleaning Procedures for Fiber Optic Connections</i> document.
The ITU signal power is too low or too high.	Check the signal power received from the OADM module. Ensure that it is between -22 dBm and -6 dBm. If not, adjust the attenuation.
The trunk fiber is broken.	Check the signal power received from the trunk. If below -22 dBm, check for trunk fiber breaks.

10.3.2 Waveethernetphy Interface Down and Shows Loss of Sync

Symptom A waveethernetphy interface is down and signal quality status shows Loss of Sync.

Table 10-1 describes the potential causes of the symptom and the solution.

Table 10-2 Waveethernetphy Interface Down and Shows Loss of Sync

Possible Problem	Solution
The optical connectors are dirty.	Refer to the <i>Cisco ONS 15530 Cleaning Procedures for Fiber Optic Connections</i> document.
The ITU signal power is too low.	Check the signal power received from the OADM module. Ensure that it is between -22 dBm and -6 dBm. If not, adjust the attenuation.
The remote client interface reported errors.	Verify that the client interface on the remote system do not report errors. Resolve any error conditions.
An interface in the signal path has errors.	Issue the show interfaces commands for the interfaces in the signal path to determine if errors occur.
The trunk fiber is broken.	Check the signal power received from the trunk. If below -22 dBm, check for trunk fiber breaks.

10.3.3 CVRD Errors on the Waveethernetphy Interface

Symptom The waveethernetphy interface is in a down state and in the **show interfaces** command output the Code violation and running disparity error count (64b66b CVRD) field are increasing and the Signal Condition field shows “Signal Fail Threshold exceeded.”

Table 10-3 describes the potential causes of the symptom and the solutions.

Table 10-3 CVRD Errors on the Waveethernetphy Interface

Possible Problem	Solution
The ITU signal power is too high or too low.	Check the signal power from the OADM module. Ensure that it is between -22 dBm and -6 dBm. If not, adjust the attenuation.
The optical connectors are dirty.	Refer to the <i>Cisco ONS 15530 Cleaning Procedures for Fiber Optic Connections</i> document.
The trunk cables are faulty.	Check the trunk fiber for pinches or breaks. Correct any problems with the fiber.
The patch cables are faulty.	Check the local patch cables between the 10-Gbps ITU tunable trunk card and the OADM module for pinches or breaks. Correct any problems with the fiber.

10.3.4 CRC and CDL HEC Errors on the Waveethernetphy Interface

Symptom The waveethernetphy interface is in a down state, the CRC error count and the CDL HEC error counts in the **show interfaces** command output is increasing, and the Signal Condition field shows “Signal Fail Threshold exceeded” or “Signal Degrade Threshold exceeded.”

Table 10-4 describes the potential causes of the symptom and the solutions.

Table 10-4 CRC and CDL HEC Errors on the Waveethernetphy Interface

Possible Problem	Solution
The data is corrupted somewhere in the data path.	<ol style="list-style-type: none"> 1. Perform a loopback on the signal path to isolate the area where the data is corrupted. For information on performing loopbacks, see the “10.4 Troubleshooting 10-Gbps ITU Tunable Trunk Card Problems Using Loopbacks” section on page 10-6. 2. Issue show interfaces commands for all the interfaces in the signal path. Resolve any error conditions or configuration problems encountered.

10.3.5 Ethernetdcc Interface Down

Symptom The ethernetdcc interface is down and pings across the interface fail.

Table 10-5 describes the potential cause of the symptom and the solution.

Table 10-5 Ethernetdcc Interface Down

Possible Problem	Solution
The ethernetdcc interface is administratively shut down.	Issue the show interfaces command to determine the administrative status of the ethernetdcc interface. If it is administratively shut down, issue the no shutdown command to bring it up.

10.4 Troubleshooting 10-Gbps ITU Tunable Trunk Card Problems Using Loopbacks

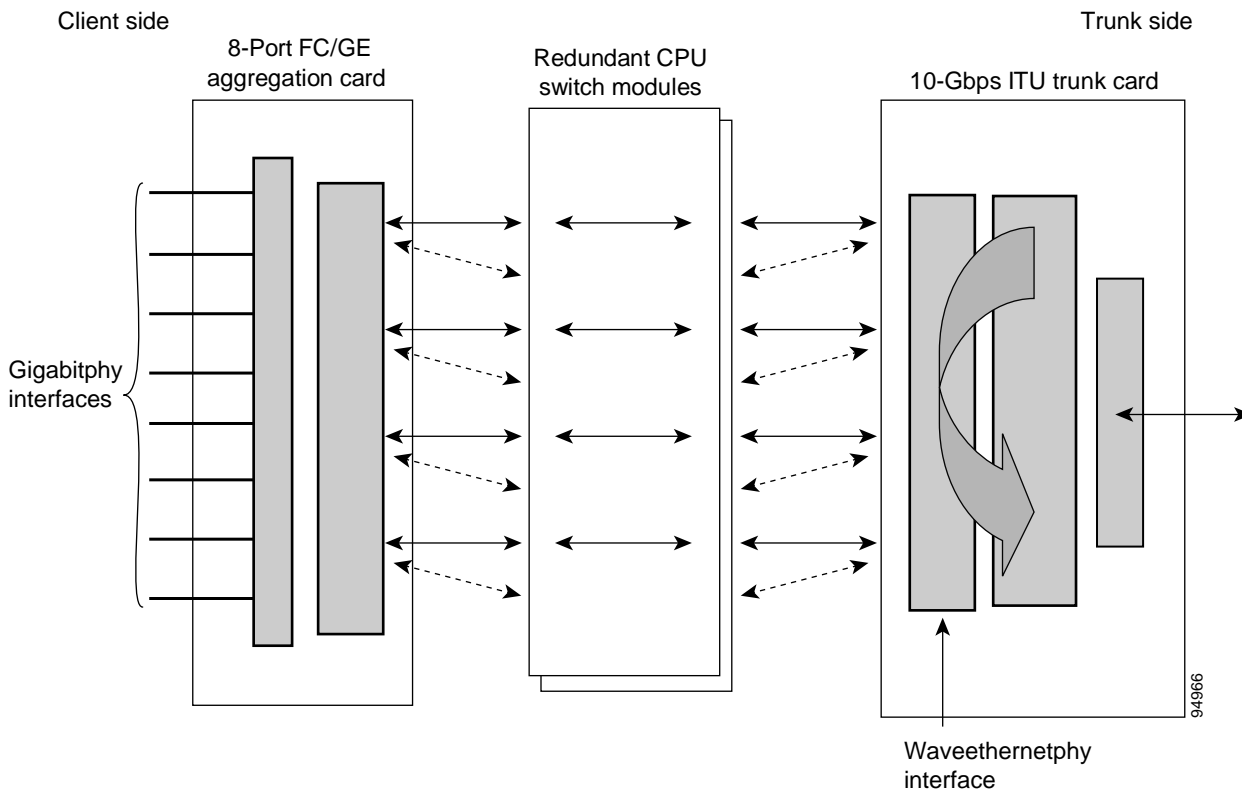
This section describes how to use software loopbacks to perform fault isolation for signals on 10-Gbps ITU tunable trunk cards. The 10-Gbps ITU tunable trunk card supports two types of software loopbacks:

- Facility loopbacks
- Terminal loopbacks

10.4.1 Facility Loopbacks

A facility loopback verifies the functioning of the 10-Gbps ITU tunable trunk card from the trunk side (see Figure 10-3).

Figure 10-3 Facility Loopback Example on a 10-Gbps ITU Tunable Trunk Card



To create a facility loopback:

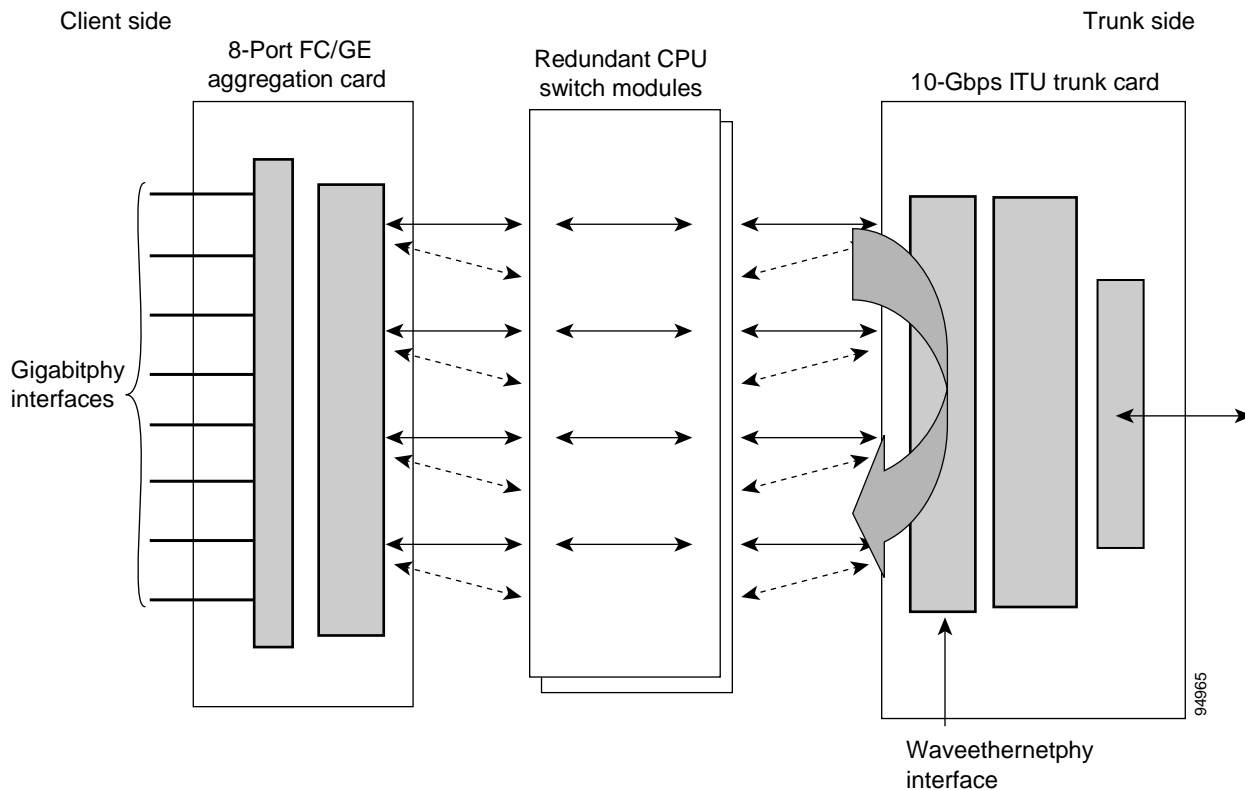
-
- Step 1** Issue a **loopback facility** command on the waveethernetphy interface.
 - Step 2** Check that the signal reaches the system at the far end.

- Step 3** If the signal does not reach the far end, check the trunk fiber and the interfaces along the signal path. If the fiber is intact, replace the card.

10.4.2 Terminal Loopbacks

A terminal loopback verifies the functioning of the 10-Gbps ITU tunable trunk card from the switch fabric side (see Figure 10-4).

Figure 10-4 Terminal Loopback Example on a 10-Gbps ITU Tunable Trunk Card



To create a terminal loopback:

- Step 1** Issue a **loopback terminal** command on the waveethernetphy interface.
- Step 2** Check that the traffic is reaching the client equipment.
- Step 3** If the signal does not reach the client equipment, replace the card.



Troubleshooting 10-Gbps Uplink Card Problems

This chapter describes how to troubleshoot 10-Gbps uplink card problems. This chapter includes the following sections:

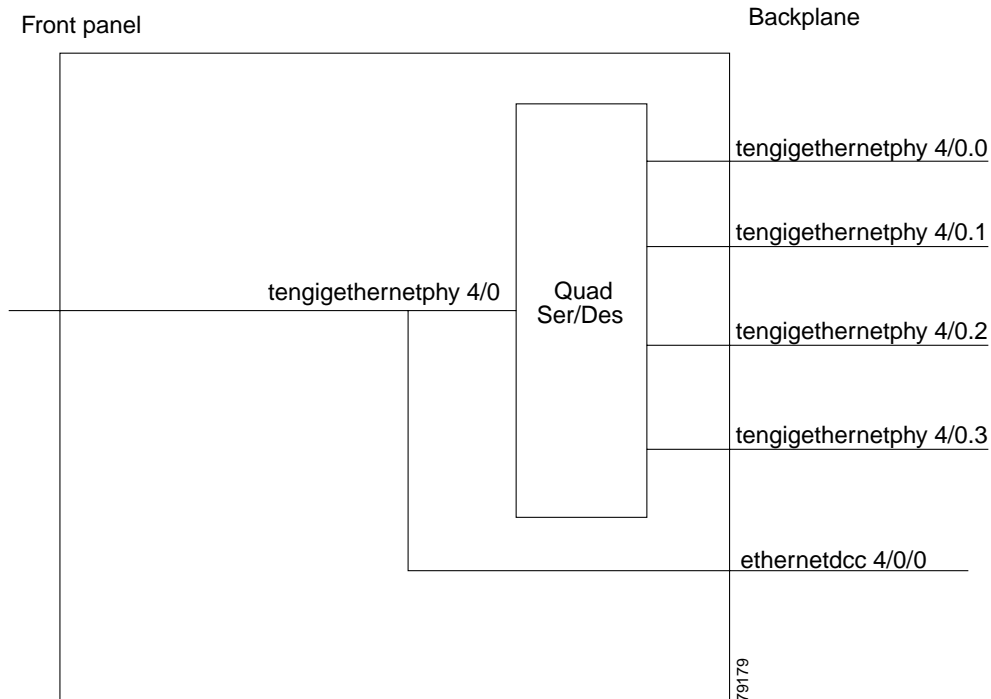
- 11.1 Overview, page 11-1
- 11.2 Initial Troubleshooting Checklist, page 11-2
- 11.3 Troubleshooting 10-Gbps Uplink Card Interface Problems, page 11-2
- 11.4 Troubleshooting 10-Gbps Uplink Card Problems Using Loopbacks, page 11-4

11.1 Overview

The 10-Gbps uplink card sends and receives a 10-Gbps 1310-nm signal to and from a 10-Gbps uplink card on another Cisco ONS 15530, or to and from a 10-GE transponder module on a Cisco ONS 15540 ESP or Cisco ONS 15540 ESPx. This card accepts up to four (3.125-Gbps line rate) electrical signals from 10-port ESCON aggregation cards and 8-port FC/GE aggregation cards and combines them into one 10-Gbps signal.

Figure 11-1 shows the interfaces for the 10-Gbps uplink card.

Figure 11-1 10-Gbps Uplink Card Interfaces



11.2 Initial Troubleshooting Checklist

Follow this initial checklist before proceeding with the troubleshooting procedures:

- Check that the receive signal power level is between -13.23 dBm and 0.5 dBm.
- Issue **show interfaces** commands to ensure that the tengigethernetphy interface is administratively up, that there are no errors on the interface, and that the laser is on.
- Issue a **show connect** command to verify the status of the cross connections to the aggregation cards.
- Check that the LEDs on the card show the proper state.
- Issue a **show facility-alarm status** command to display the alarms on the interfaces.
- Ensure that all optical connectors are clean. Refer to the *Cisco ONS 15530 Cleaning Procedures for Fiber Optic Connections* document.

11.3 Troubleshooting 10-Gbps Uplink Card Interface Problems

This section contains troubleshooting procedures for 10-Gbps uplink card interface problems.

11.3.1 Tengigethernephy Interface Down and Shows Loss of Lock

Symptom A tengigethernephy interface is down and the signal quality status shows Loss of Lock.

Table 11-1 describes the potential causes of the symptom and the solutions.

Table 11-1 *Tengigethernephy Interface Down and Shows Loss of Lock*

Possible Problem	Solution
The optical connectors are dirty.	Refer to the <i>Cisco ONS 15530 Cleaning Procedures for Fiber Optic Connections</i> document.
The receive signal power is too low or too high.	Check the receive signal power. Ensure that it is between -13.23 dBm and 0.5 dBm. If not, adjust the attenuation.
The fiber is broken.	Check the receive signal power received. If below -13.23 dBm, check for fiber breaks.

11.3.2 Tengigethernephy Interface Down and Shows Loss of Sync

Symptom A tengigethernephy interface is down and the signal quality status shows Loss of Sync.

Table 11-2 describes the potential cause of the symptom and the solution.

Table 11-2 *Tengigethernephy Interface Down and Shows Loss of Sync*

Possible Problem	Solution
The optical connectors are dirty.	Refer to the <i>Cisco ONS 15530 Cleaning Procedures for Fiber Optic Connections</i> document.
The receive signal power is too low.	Check the receive signal power received. Ensure that it is between -13.23 dBm and 0.5 dBm. If not, adjust the attenuation.

11.3.3 Ethernetdcc Interface Down

Symptom The ethernetdcc interface is down and pings across the interface fail.

Table 11-3 describes the potential cause of the symptom and the solution.

Table 11-3 *Ethernetdcc Interface Down*

Possible Problem	Solution
The ethernetdcc interface is administratively shut down.	Issue the show interfaces command to determine the administrative status of the ethernetdcc interface. If it is administratively shut down, issue the no shutdown command to bring it up.

11.4 Troubleshooting 10-Gbps Uplink Card Problems Using Loopbacks

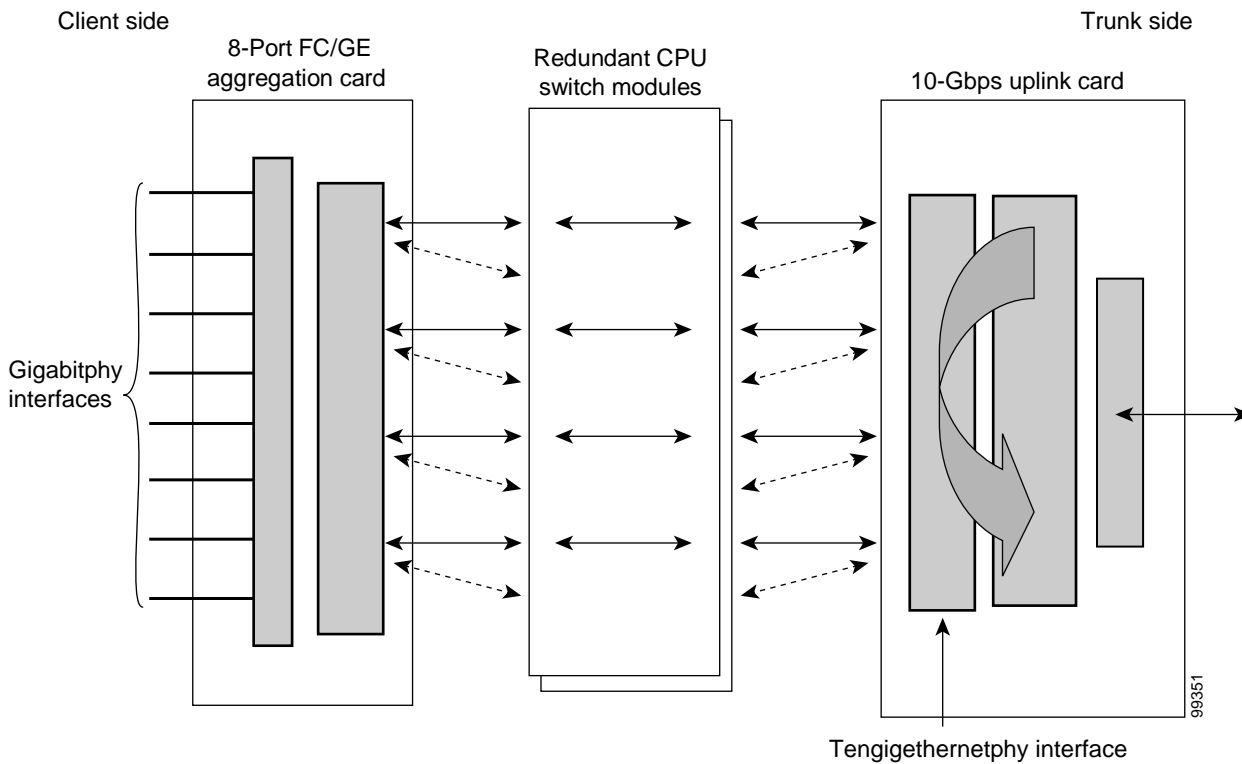
This section describes how to use software loopbacks to perform fault isolation for signals on 10-Gbps uplink cards. The 10-Gbps uplink card supports two types of software loopbacks:

- Facility loopbacks
- Terminal loopbacks

11.4.1 Facility Loopbacks

A facility loopback verifies the functioning of the 10-Gbps uplink card from the trunk side (see Figure 11-2).

Figure 11-2 Facility Loopback Example on a 10-Gbps Uplink Card



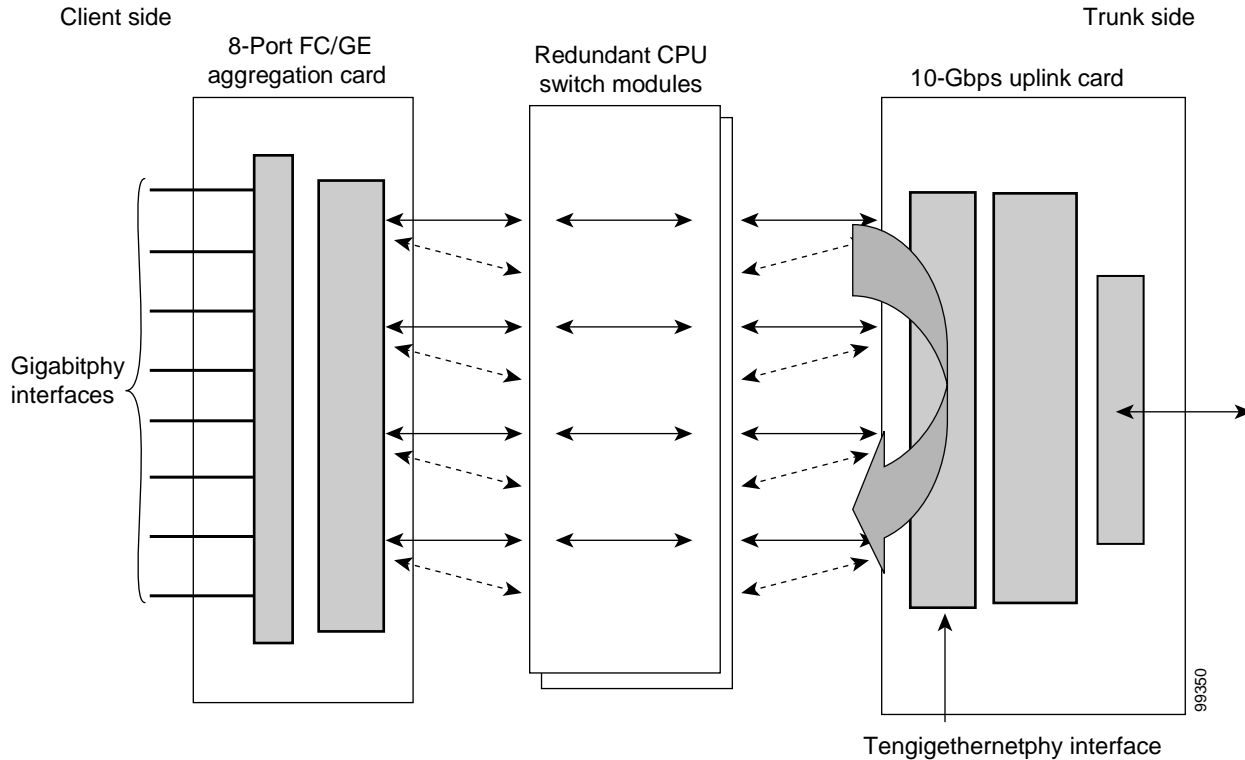
To create a facility loopback:

-
- Step 1** Issue a **loopback facility** command on the tenGigetherethy interface.
 - Step 2** Check that the signal reaches the system at the far end.
 - Step 3** If the signal does not reach the far end, check the trunk fiber and the interfaces along the signal path. If the fiber is intact, replace the card.
-

11.4.2 Terminal Loopbacks

A terminal loopback verifies the functioning of the 10-Gbps uplink card from the switch fabric side (see Figure 11-3).

Figure 11-3 Terminal Loopback Example on a 10-Gbps Uplink Card



To create a terminal loopback:

-
- Step 1** Issue a **loopback terminal** command on the tengigethernetphy interface.
 - Step 2** Check that the traffic is reaching the client equipment.
 - Step 3** If the signal does not reach the client equipment, replace the card.
-



Troubleshooting OADM Module Problems

This chapter describes how to troubleshoot OADM module problems. This chapter includes the following sections:

- 12.1 Overview, page 12-1
- 12.2 Initial Troubleshooting Checklist, page 12-2
- 12.3 Troubleshooting OADM Module Problems, page 12-3

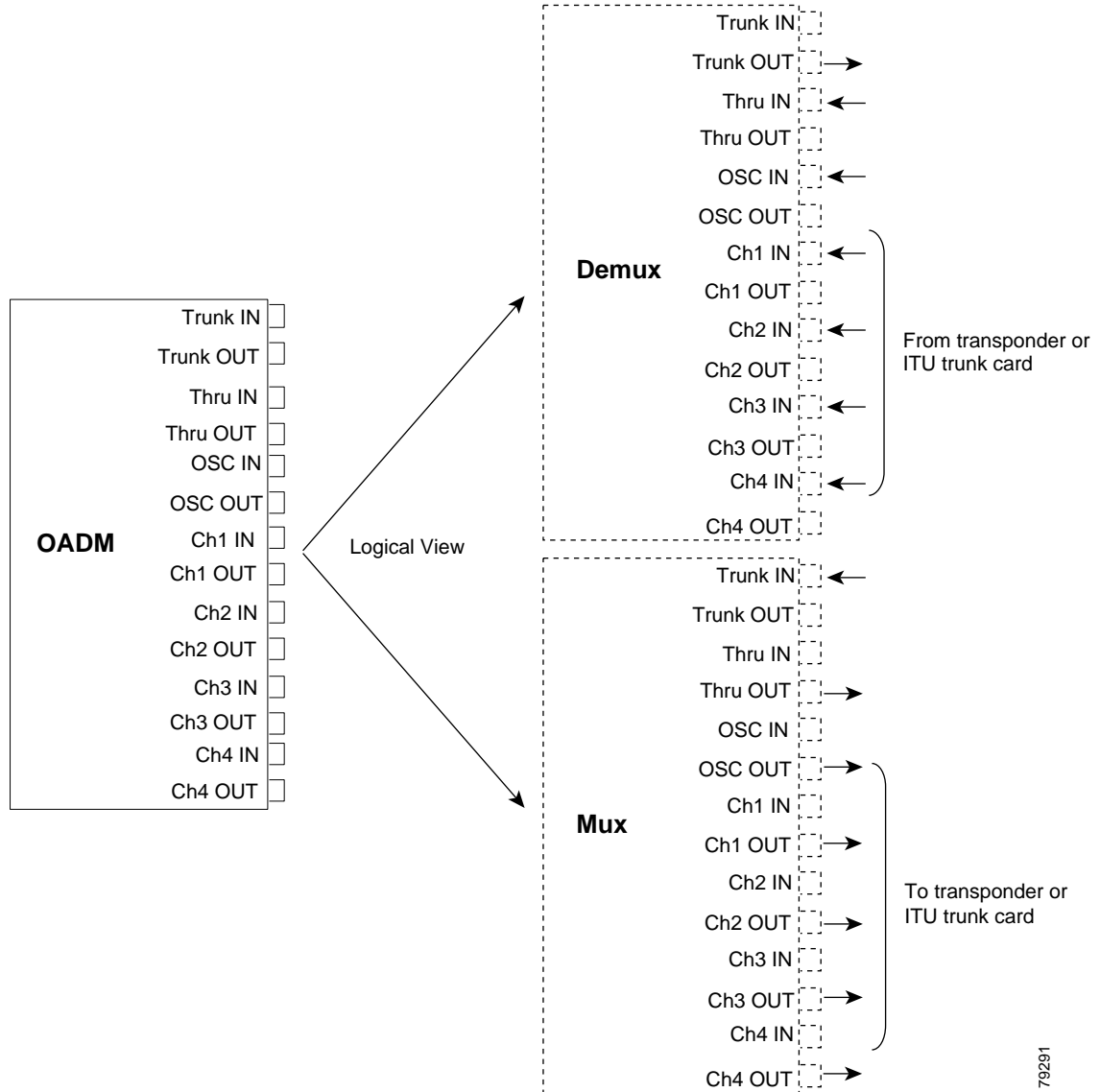
12.1 Overview

The OADM (optical add/drop multiplexer) modules are passive devices that optically multiplex and demultiplex a specific band of four ITU wavelengths. The OADM modules supported by the Cisco ONS 15530 each add and drop a band of channels at a node and pass the other bands through. To support the 32-channel spectrum, there are eight different 4-channel OADM modules, each supporting a different band of channels.

In the transmit direction, the OADM modules multiplex signals transmitted by the line cards over optical cross connections and provide the interfaces to connect the multiplexed signal to the DWDM trunk side. In the receive direction, the OADM modules demultiplex the signals from the trunk side before passing them over optical cross connections to the line cards.

Figure 12-1 shows the physical layout of the OADM module for the channels in band A (1–4) along with a logical view of its multiplexing and demultiplexing functions. Optical signals received from the line card, the Thru IN connector, and the OSC IN connector are multiplexed and sent through the Trunk OUT connector. The optical signal received from the Trunk IN connector is demultiplexed and the OSC signal is sent to the OSC OUT connector; the dropped channels are sent to the line card; and the passed channels are sent to the Thru OUT connector.

Figure 12-1 OADM Module Architecture



12.2 Initial Troubleshooting Checklist

Follow this initial checklist before proceeding with the troubleshooting procedures:

- Issue a **show interfaces** command to ensure that the OADM channel interfaces are administratively up, that there are no errors on the interfaces, and that the laser frequency is correctly configured.
- Issue a **show optical filter** command to verify the configuration of the channels of the OADM interfaces.
- Issue a **show connect intermediate** command to verify the status of the wavepatch interface connected to the OADM module.
- Issue a **show facility-alarm status** command to display the alarms on the interfaces.

- Check that the trunk cards and transponder line cards are patched to the correct OADM ports. Issue a **show patch** command to verify that there are no frequency mismatches.
- Ensure that all optical connectors are clean. Refer to the *Cisco ONS 15530 Cleaning Procedures for Fiber Optic Connections* document.

12.3 Troubleshooting OADM Module Problems

This section contains troubleshooting procedures for OADM module problems.

12.3.1 OADM Module Is Not Recognized

Symptom The OADM module does not appear in the **show interfaces** or the **show running-config** command output.

Table 12-1 describes the potential causes of the symptom and the solutions.

Table 12-1 OADM Module Not Recognized

Possible Problem	Solution
OADM module is not inserted properly.	Remove and carefully reinsert the OADM module. Issue a show interfaces command or the show running-config command to ensure that the OADM channel interfaces are up.

12.3.2 OADM Channel Interfaces Are Not Recognized After a CPU Switch Module Switchover

Symptom OADM channel interfaces are not recognized after a CPU switch module switchover.

Table 12-2 describes the potential causes of the symptom and the solutions.

Table 12-2 OADM Channel Interfaces Not Recognized After Switchover

Possible Problem	Solution
OADM module IDPROM not programmed correctly.	Issue a show running-config command to verify that the OADM channel interfaces are present. Repeat on the standby side. If the interfaces are not present, call Cisco customer support.

12.3.3 Waveethernetphy or Wave Interface Is Down

Symptom The waveethernetphy or the wave interface on the connected transponder is down.

Table 12-3 describes the potential causes of the symptom and the solutions.

Table 12-3 *Waveethernetphy or Wave Interface Is Down*

Possible Problem	Solution
Patch cables incorrectly connected.	Issue a show patch command and check the output for errors. If errors appear, move the patch cable to the correct port.
Patch cables are defective.	Visually inspect the patch cables. Replace the patch cables if necessary.



Troubleshooting PSM Problems

This chapter describes how to troubleshoot PSM problems. This chapter includes the following sections:

- 13.1 Overview, page 13-1
- 13.2 Initial Troubleshooting Checklist, page 13-1
- 13.3 Troubleshooting PSM Interface Problems, page 13-1

13.1 Overview

The PSM (protection switch module) provides trunk fiber protection for Cisco ONS 15530 systems configured in point-to-point topologies. The PSM sends the signal from an OADM module, a transponder line card, or an ITU trunk card to both the west and east directions. It receives both the west and east signals and selects one to send to the OADM module, the transponder line card, or ITU trunk card. When a trunk fiber cut occurs on the active path, the PSM switches the received signal to the standby path. The PSM can protect up to 32 data channels and the OSC.

The PSM also has an optical monitor port for testing the west and east receive signals. This port samples one percent of the receive signals that can be monitored with an optical power meter.

13.2 Initial Troubleshooting Checklist

Follow this initial checklist before proceeding with the troubleshooting procedures:

- Check that the LEDs on the cards show the proper state.
- Verify patch configuration.
- Ensure that all optical connectors are clean. Refer to the *Cisco ONS 15530 Cleaning Procedures for Fiber Optic Connections* document.

13.3 Troubleshooting PSM Interface Problems

This section contains troubleshooting procedures for PSM interface problems.

13.3.1 Wdmsplit Interface Down

Symptom The wdmsplit interface is down.

Table 13-1 describes the potential causes of the symptom and the solutions.

Table 13-1 *Wdmsplit Interface Is Down*

Possible Problem	Solution
Interface administratively shut down.	Issue the show interfaces wdmsplit command to ensure the interface is active. If necessary, issue the no shutdown command to activate the interface.
Incoming power level is out of range.	Use a power meter to check the receive power level from the remote node. Issue the show interfaces wdmsplit command to verify the power level is within range.
The optical connectors are dirty.	Refer to the <i>Cisco ONS 15530 Cleaning Procedures for Fiber Optic Connections</i> document.

13.3.2 Wdmsplit Interface Power Level Indicates Loss of Light

Symptom The wdmsplit interface is down and shows Loss of Light.

Table 13-2 describes the potential causes of the symptom and the solutions.

Table 13-2 *Wdmsplit Interface Power Level Indicates Loss of Light*

Possible Problem	Solution
Incorrect cable connection.	Verify that the optical cables are connected correctly.
Incoming power level is low.	Issue the show interfaces wdmsplit command to verify the receive power level is within range.
The optical connectors are dirty.	Refer to the <i>Cisco ONS 15530 Cleaning Procedures for Fiber Optic Connections</i> document.

13.3.3 Wdmsplit Interface Receives Light But End Wave Interface Shows Loss of Light

Symptom The wdmsplit interface receives light but the end wave interface shows Loss of Light.

Table 13-3 describes the potential causes of the symptom and the solutions.

Table 13-3 *Wdmsplit Interface Receives Light But End Wave Interface Shows Loss of Light*

Possible Problem	Solution
The patch between the wdmrelay interface and the wdm or wavepatch interface is incorrect.	Issue the show patch and show interfaces wdm commands to verify that the patch is correctly configured.
The patch between the OADM module and the line card is incorrect.	Verify that the patch cables are connected correctly between the OADM module and the line card.
The optical connectors are dirty.	Refer to the <i>Cisco ONS 15530 Cleaning Procedures for Fiber Optic Connections</i> document.

13.3.4 Wdm Interface Loses Topology Neighbor Learning Via CDP

Symptom The wdm interface loses topology neighbor learning through CDP after the patch between the wdmrelay and wdm interfaces is configured.

Table 13-4 describes the potential cause of the symptom and the solution.

Table 13-4 *Wdm Interface Loses Topology Neighbor Learning Via CDP*

Possible Problem	Solution
The patch between the wdmrelay interface and the wdm or wavepatch interface is incorrect	Issue the show patch and show interfaces wdm commands to verify that the patch is correctly configured. Once this patch is configured, the trunk side interface is no longer an edge interface so topology learning through CDP is disabled.

13.3.5 Automatic CDP Learning Is Not Enabled on Wdmsplit Interface

Symptom Automatic CDP learning is not enabled on the wdmsplit interfaces after a patch between the wdmrelay and wdm interfaces is configured.

Table 13-5 describes the potential cause of the symptom and the solution.

Table 13-5 *Automatic CDP Learning Is Not Enabled on Wdmsplit Interface*

Possible Problem	Solution
N/A	Neighbor information must be manually configured. Topology learning through CDP is not supported on wdmsplit interfaces.

■ 13.3.5 Automatic CDP Learning Is Not Enabled on Wdm-split Interface



Troubleshooting VOA Module Problems

This chapter describes how to troubleshoot problems with VOA modules on the Cisco ONS 15530.

This chapter includes the following sections:

- 14.1 Overview, page 14-1
- 14.2 Initial Troubleshooting Checklist, page 14-3
- 14.3 Troubleshooting VOA Module Problems, page 14-3

14.1 Overview

The VOA modules are half-width modules inserted into a carrier motherboard installed in a Cisco ONS 15530 shelf. The carrier motherboards can be installed in slots 1 through 4 and 7 through 10. Each carrier motherboard can hold up to two VOA modules. The Cisco ONS 15530 supports four types of VOA modules:

- Single WB-VOA modules
- Dual WB-VOA modules
- Single band PB-OE modules
- Dual band PB-OE modules

Figure 14-1 shows an example of the interfaces for a single WB-VOA module.

Figure 14-1 *Single WB-VOA Module Interfaces*

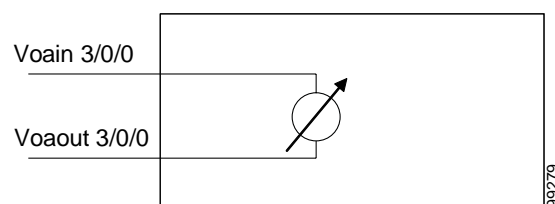


Figure 14-2 shows an example of the interfaces for a dual WB-VOA module.

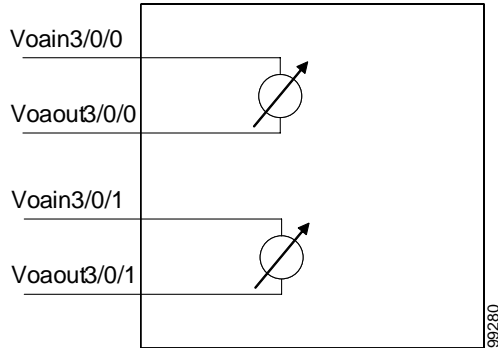
Figure 14-2 *Dual WB-VOA Module Interfaces*

Figure 14-3 shows an example of the interfaces for a single PB-OE module.

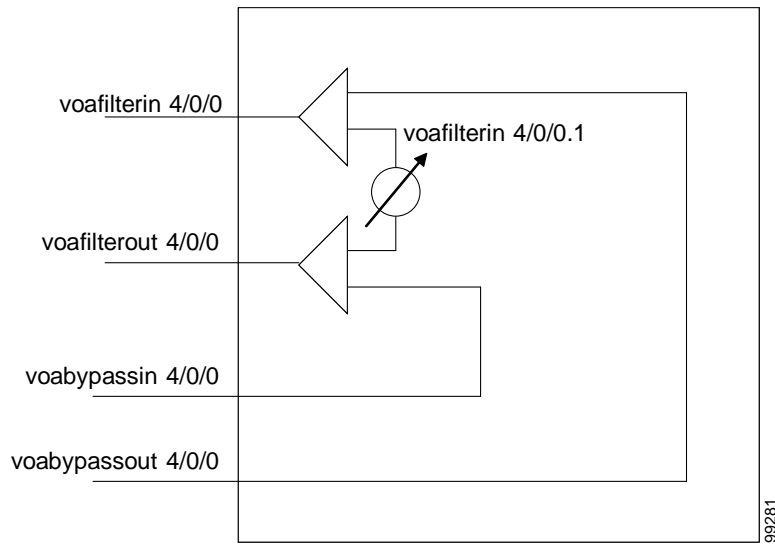
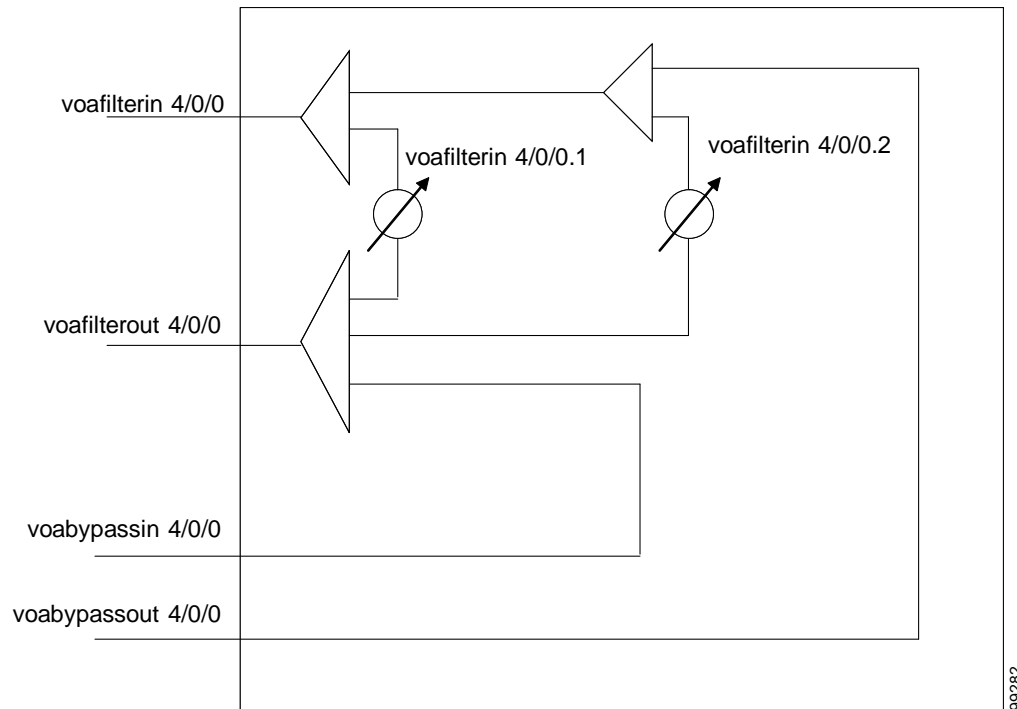
Figure 14-3 *Single PB-OE Module Interfaces*

Figure 14-4 shows an example of the interfaces for a dual PB-OE module.

Figure 14-4 Dual PB-OE Module Interfaces



14.2 Initial Troubleshooting Checklist

Follow this initial checklist before proceeding with the troubleshooting procedures:

- Check that the receive signal power is between -28 dBm and 11 dBm for WB-VOA modules and between -26 dBm and 11 dBm for PB-OE modules.
- Issue **show interfaces** commands to verify that the values of the optical receive thresholds are set to the desired tenths of decibels.
- Check that the LEDs on the modules show the proper state.
- Issue a **show facility-alarm status** command to display the alarms on the interfaces.
- Check that the VOA modules are patched correctly. Issue a **show patch** command to verify that the patch configuration is correct.
- Ensure that all optical connectors are clean. Refer to the *Cisco ONS 15530 Cleaning Procedures for Fiber Optic Connections*.

14.3 Troubleshooting VOA Module Problems

This section contains troubleshooting procedures for VOA module interface problems.

14.3.1 Voain Interface Shows Low Optical Alarm Threshold Error

Symptom The power of the signal monitored by the voain interface on a WB-VOA interface crossed the low optical alarm threshold value and the system raised an alarm.

Table 14-1 describes the potential causes of the symptom and the solutions.

Table 14-1 Voain Interface Shows Low Optical Alarm Threshold Error

Possible Problem	Solution
The signal is overattenuated.	<ol style="list-style-type: none"> 1. Issue a show interfaces command on the voain interface to verify the attenuation setting. 2. Use an OPM (optical power monitor) to determine the signal power. 3. Issue an optical attenuation command to reduce the attenuation. <p>For more information on setting attenuation values, refer to the <i>Cisco ONS 15530 Optical Transport Turn-Up and Test Guide</i>.</p>
The signal power is too low due to a failure in the signal path.	<ol style="list-style-type: none"> 1. Issue show interfaces commands for the interfaces in the signal path. 2. Resolve any interface problems detected.
The attenuation is set too high.	<ol style="list-style-type: none"> 1. Issue a show interfaces command on the voain interface to verify the attenuation setting. 2. Issue an optical attenuation command to reduce the attenuation.
The optical connectors are dirty.	Refer to the <i>Cisco ONS 15530 Cleaning Procedures for Fiber Optic Connections</i> document.

14.3.2 Voafilterin Subinterface Shows Low Optical Alarm Threshold Error

Symptom The power of the signal monitored by the voafilterin subinterface on a PB-OE module crossed the low optical alarm threshold value and the system raised an alarm.

Table 14-2 describes the potential causes of the symptom and the solutions.

Table 14-2 Voafilterin Subinterface Shows Low Optical Alarm Threshold Error

Possible Problem	Solution
The signal is overattenuated.	<ol style="list-style-type: none"> 1. Issue a show interfaces command on the voafilterin subinterface to verify the attenuation setting. 2. Use an OPM (optical power monitor) to determine the signal power. 3. Issue an optical attenuation command to reduce the attenuation.
The PB-OE module does not support the channel bands on the trunk signal.	<ol style="list-style-type: none"> 1. Check the network design to verify that the channel band attenuated by the PB-OE module is present. 2. If channel band is not present, obtain the correct PB-OE module.
The optical connectors are dirty.	Refer to the <i>Cisco ONS 15530 Cleaning Procedures for Fiber Optic Connections</i> document.

14.3.3 Voain Interface Shows High Optical Alarm Threshold Error

Symptom The power of the signal monitored by the voain interface on a WB-VOA module crossed the high optical alarm threshold value and the system raised an alarm.

Table 14-3 describes the potential causes of the symptom and the solutions.

Table 14-3 Voain Interface Shows High Optical Alarm Threshold Error

Possible Problem	Solution
The signal attenuation is too low.	<ol style="list-style-type: none"> 1. Issue a show interfaces command on the voain interface to verify the attenuation setting. 2. Use an OPM (optical power monitor) to determine the signal power. 3. Issue an optical attenuation command to increase the attenuation. <p>For more information on setting attenuation values, refer to the <i>Cisco ONS 15530 Optical Transport Turn-Up and Test Guide</i>.</p>
The high alarm threshold value is set too low.	<ol style="list-style-type: none"> 1. Issue a show interfaces command on the voain interface to verify the threshold setting. 2. Issue an optical threshold command to increase the threshold setting.

14.3.4 Voafilterin Subinterface Shows High Optical Alarm Threshold Error

Symptom The power of the signal monitored by the voafilterin subinterface on a PB-OE module crossed the high optical alarm threshold value and the system raised an alarm.

Table 14-4 describes the potential causes of the symptom and the solutions.

Table 14-4 Voafilterin Subinterface Shows High Optical Alarm Threshold Error

Possible Problem	Solution
The signal attenuation is too low.	<ol style="list-style-type: none"> 1. Issue a show interfaces command on the voafilterin subinterface to verify the attenuation setting. 2. Use an OPM (optical power monitor) to determine the signal power. 3. Issue an optical attenuation command to increase the attenuation. <p>For more information on setting attenuation values, refer to the <i>Cisco ONS 15530 Optical Transport Turn-Up and Test Guide</i>.</p>
The high alarm threshold value is set too low.	<ol style="list-style-type: none"> 1. Issue a show interfaces command on the voafilterin subinterface to verify the threshold setting. 2. Issue an optical threshold command to increase the threshold setting.

14.3.5 STA LED Continues Blinking After Initialization Complete

Symptom The STA LED continues to blink after initialization of the VOA module should be complete. For removal and reinsertion, initialization completes in a few seconds. For system reload, initialization completes after the entire shelf is initialized.

Table 14-5 describes the potential causes of the symptom and the solutions.

Table 14-5 **STA LED Continues Blinking After Initialization Complete**

Possible Problem	Solution
The VOA module is not properly seated.	Remove and reinsert the VOA module as described in the <i>Cisco ONS 15530 Optical Transport Turn-Up and Test Guide</i> .
The carrier motherboard is not properly seated.	<ol style="list-style-type: none"> 1. Remove the VOA module as described in the <i>Cisco ONS 15530 Optical Transport Turn-Up and Test Guide</i>. 2. Reseat the carrier motherboard. 3. Reinsert the VOA module as described in the <i>Cisco ONS 15530 Optical Transport Turn-Up and Test Guide</i>.

14.3.6 Optical Threshold Warnings Not Reported

Symptom The signal power crosses an optical warning threshold and it is not reported.

Table 14-6 describes the potential cause of the symptom and the solution.

Table 14-6 **Optical Threshold Warnings Not Reported**

Possible Problem	Solution
The optical warnings are configured to not be reported.	<ol style="list-style-type: none"> 1. Issue a show interfaces command on the voain interface or the voafilterin subinterface. 2. Issue an optical threshold command if the optical warning threshold severity is set to not reported. Change the severity to minor or not alarmed.



Troubleshooting APS Problems

This chapter describes how to troubleshoot APS (Automatic Protection Switching) problems. This chapter includes the following sections:

- 15.1 Overview, page 15-1
- 15.2 Initial Troubleshooting Checklist, page 15-1
- 15.3 Troubleshooting Specific APS Problems, page 15-2

15.1 Overview

APS provides protection against signal transmission failure. The Cisco ONS 15530 supports the following APS features:

- 1+1 path protection
- Splitter protection
- Line card protection
 - Client based
 - Y-cable based
 - Switch fabric based
- Trunk fiber protection
- Redundant switch fabric protection
- Bidirectional and unidirectional path switching

For more information on APS support on the Cisco ONS 15530, refer to the *Cisco ONS 15530 Configuration Guide*.

15.2 Initial Troubleshooting Checklist

Follow this initial checklist before proceeding with the troubleshooting procedures:

- Issue **show interfaces** commands to ensure that the interfaces along the signal paths are administratively up and that there are no errors on the interfaces.
- Issue a **show connect** command to verify the status of the cross connections.
- Issue a **show aps detail** command on both nodes to verify the following:

- The working and protection interfaces are correct.
- The `aps state` field shows “enabled (associated).”
- The `msg-channel` field shows “Up” on the desired message channel.
- The `direction` field shows the same expected values (either “uni” or “bi”) on both nodes.
- Check that the LEDs on the cards show the proper state.
- Issue a **show facility-alarm status** command to display the alarms on the interfaces.
- If ITU cards are present, check that the ITU cards are patched to the correct OADM ports. Issue a **show patch detail** command to verify that there are no frequency mismatches.
- Ensure that all optical connectors are clean. Refer to the *Cisco ONS 15530 Cleaning Procedures for Fiber Optic Connections* document.

15.3 Troubleshooting Specific APS Problems

This section contains troubleshooting information for specific APS problems.

15.3.1 APS Group State Enabled But Not Associated

Symptom The **show aps group** command or **show aps detail** command output show an APS group state is enabled but the group is not associated.

Table 15-1 describes the potential causes of the symptoms and the solutions.

Table 15-1 APS Group State Enabled But Not Associated

Possible Problem	Solution
Either the working or protection channel is not present.	Make sure that all the cards are properly seated and that the LEDs are showing the proper state.
For switch fabric based line card protection, the cross connections through the switch fabric are not configured correctly.	<ol style="list-style-type: none"> 1. Issue a show connect command to verify that the working and protection cross connections are correctly configured. 2. Issue the connect command to correct any problems.

15.3.2 Bidirectional APS Configured But Remote Node Direction, Architecture, and Receive k1/k2 Are Unknown

Symptom The **show aps group** command or the **show aps detail** command output shows an APS group state is configured for bidirectional switching but the remote node direction, remote node architecture, and receive k1/k2 are unknown.

Table 15-2 describes the potential causes of the symptoms and the solutions.

Table 15-2 Bidirectional APS Configured But Remote Node Direction, Architecture, and Receive k1/k2 Are Unknown

Possible Problem	Solution
The configured message channel is not up (if the message channel is not IP).	<ol style="list-style-type: none"> 1. Issue a show interfaces wave command or a show interfaces ethernetdcc command to check the status of the message channel interface. 2. If both the interface and the line protocol are down check the trunk fiber and the local and remote patched fibers to ensure that light is received on the message channel interface. 3. If the interface is up but the protocol is down, issue the debug oscp hello-packet command to determine whether OSCP Hello packets are received from and transmitted to the far end.
There is a problem with OSCP.	See Chapter 16, “Troubleshooting OSCP Problems.”
The client signal has errors.	Issue the show interfaces command to check the error counters on the active interface. If they are increasing, the line could be bad.

15.3.3 Message Channel Interface Up But APS Msg-Channel Status Down

Symptom The configured message channel interface is up but the msg-channel status in the **show aps group** or **show aps detail command** output is down.

Table 15-3 describes the potential causes of the symptoms and the solutions.



Note

Check both the local and remote systems for message channel problems.

Table 15-3 Message Channel Interface Up But APS msg-channel Status Down

Possible Problem	Solution
The line cards are not correctly patched to the OADM modules.	Check the patch connections on the shelf. Ensure that ITU trunk cards are connected to the correct filter ports on the OADM module.
The OSC modules are not correctly patched to the OADM modules.	Check that the OSC module is correctly patched to the OADM module.
The laser frequency on the 2.5-Gbps ITU trunk card is not configured correctly.	Issue a show interfaces command to verify that the laser frequency is correctly configured on the transponder line cards and the 2.5-Gbps ITU trunk cards. If not, issue a laser frequency command to configure the correct laser frequency.
The patches between the line cards or the OSC modules and the OADM modules are not configured in the CLI.	Issue a show patch command to verify the patch connections are correctly configured. If not, issue the patch command to correct the configuration.

Table 15-3 Message Channel Interface Up But APS msg-channel Status Down (continued)

Possible Problem	Solution
The unused wavepatch on a splitter line card in a line card protected configuration is not disabled.	Issue the shutdown command to disable the unused wavepatch interfaces.
If far-end group names are used in the APS message channel configuration, the names are not configured correctly.	<ol style="list-style-type: none"> 1. Issue the show aps group command or the show aps detail command to verify the far-end group name configuration. 2. Issue the aps message-channel command to correct the far-end group name configuration.
The message channel is IP and the NME ¹ connection is down.	Issue the show interfaces fastethernet 0 command to verify the status of the NME. If the line or the protocol is down, see Chapter 2, “Troubleshooting CPU Switch Module Problems.”
The optical connectors are dirty.	Refer to the <i>Cisco ONS 15530 Cleaning Procedures for Fiber Optic Connections</i> document.

1. NME = network management Ethernet

15.3.4 APS Does Not Switch to Protection Signal When the Working Signal Fails

Symptom When the working signal fails, APS does not switch over to the protection signal.

Table 15-4 describes the potential causes of the symptoms and the solutions.

Table 15-4 APS Does Not Switch to Protection Signal When the Working Signal Fails

Possible Problem	Solution
An APS switchover request is pending.	<ol style="list-style-type: none"> 1. Issue the show aps group command or the show aps detail command to determine the pending APS request. 2. Issue the aps clear command to remove the APS request.
A trunk failure occurred on the protection signal.	Correct the failure on the protection signal. See Chapter 3, “Troubleshooting Transponder Line Card Problems,” Chapter 8, “Troubleshooting 2.5-Gbps ITU Trunk Card Problems,” Chapter 9, “Troubleshooting 10-Gbps ITU Trunk Card Problems.” or Chapter 10, “Troubleshooting 10-Gbps ITU Tunable Trunk Card Problems.”

15.3.5 Lockout from Protection Request Fails

Symptom A request to lock out an APS switchover to the protection path made with an **aps lockout** command failed.

Table 15-5 describes the potential cause of the symptom and the solution.

Table 15-5 Lockout from Protection Request Fails

Possible Problem	Solution
The active signal is already switched to the protection path.	<ol style="list-style-type: none"> 1. Issue the aps switch group-name force protection-to-working command to ensure that the active signal is on the working path and then Issue the aps lockout command. 2. If the aps switch group-name force protection-to-working command fails, check the status of the working path using the show interfaces command and resolve the signal failure.

15.3.6 Several Unexpected APS Messages Received

Symptom Several unexpected APS messages display on the console.

Table 15-6 describes the potential cause of the symptom and the solution.

Table 15-6 Several Unexpected APS Messages Received

Possible Problem	Solution
A bidirectional APS group on one end is enabled and disabled while the other end is generating a high priority request.	Issue an aps enable/no aps enable command sequence to reinitialize the message channel. This is a temporary condition and should disappear when both ends reestablish APS communication.

15.3.7 Remote Switchover Does Not Occur After Local Switchover

Symptom The remote system does not switch over after the local system switches over.

Table 15-7 describes the potential causes of the symptoms and the solutions.

Table 15-7 Remote Switchover Does Not Occur After Local Switchover

Possible Problem	Solution
Both systems are not configured for bidirectional APS.	<ol style="list-style-type: none"> 1. Issue show aps detail commands on both systems to verify the APS direction configuration. 2. Issue aps direction commands to correct the APS direction configuration, if necessary.
The protection path on the remote system has failed.	<ol style="list-style-type: none"> 1. Issue a show interfaces command for the protection interface on the remote system. 2. Resolve any problems on the interface.

15.3.8 Manual or Forced Switchover Fails

Symptom A request for a manual or forced APS switchover fails.

Table 15-8 describes the potential cause of the symptom and the solution.

Table 15-8 *Manual or Forced Switchover Fails*

Possible Problem	Solution
A higher priority request is in effect. For bidirectional APS, the higher priority request might originate from the remote node.	<ol style="list-style-type: none"> 1. Issue the show aps group command or the show aps detail command to determine if the request is user generated or system generated. 2. For user generated requests, issue the aps clear command to remove the higher priority request. 3. For system generated requests, correct the failure that is preventing the switchover.

15.3.9 Wave Interface or Waveethernetphy Interface Is Down and One Wavepatch Interface Is Up

Symptom Wave interface or waveethernetphy interface is down and one of the wavepatch interfaces is up when the APS group is bidirectional.

Table 15-9 describes the potential causes of the symptoms and the solutions.

Table 15-9 *Wave Interface or Waveethernetphy Interface Is Down and One Wavepatch Interface Is Up*

Possible Problem	Solution
A signal failure occurred on the receive side of the working path on the local system.	Correct the signal failure on the local system.
A signal failure occurred on the receive side of the protection path of the remote system.	Correct the signal failure on the remote system.

15.3.10 APS Group Transmitting k1k2 sf-lp to Peer APS Group

Symptom The transmit k1k2 field in the **show aps group** or **show aps detail** command output indicates sf-lp is sent to the peer APS group in a y-cable configuration.

Table 15-10 describes the potential causes of the symptoms and the solutions.

Table 15-10 APS Group Transmitting k1k2 sf-lp to Peer APS Group

Possible Problem	Solution
A trunk fiber break or misconfiguration is causing keepalive timeouts.	<ol style="list-style-type: none"> 1. Check the show facility status command output for keepalive timeout alarms on the active interface. 2. Verify that there are no breaks on the trunk fiber. 3. Issue show interfaces commands on the active interfaces on the system to verify that the flow identifier is correctly configured. Issue the cdl flow identifier command to correct mismatches.
A fiber break is causing Tx-CRC threshold alarms.	<ol style="list-style-type: none"> 1. Check the show facility status command output for Tx-CRC alarms on the active interface. 2. Verify that there are no breaks on the trunk or client fiber.
A failure occurred on the client receive signal.	<ol style="list-style-type: none"> 1. Check the show facility status command output for loss of signal and loss of sync alarms on the active interface. 2. Verify that there are no breaks on the client fiber and that the connector are clean. Refer to the <i>Cisco ONS 15530 Cleaning Procedures for Fiber Optic Connections</i> document. 3. Ensure that the SFP optics are properly seated and that the LEDs are on. 4. Issue a show interfaces command to verify the protocol encapsulation. Issue the encapsulation command to correct any misconfiguration.

■ 15.3.10 APS Group Transmitting k1k2 sf-lp to Peer APS Group



Troubleshooting OSCP Problems

This chapter describes how to troubleshoot OSCP problems. This chapter includes the following sections:

- 16.1 Overview, page 16-1
- 16.2 Initial Troubleshooting Checklist, page 16-1
- 16.3 Troubleshooting OSCP Problems, page 16-1

16.1 Overview

The OSC (optical supervisory channel) module supports an optional out-of-band management channel for communicating between systems on the network. The OSC (channel 0) allows control and management traffic to be carried without requiring a separate Ethernet connection to each Cisco ONS 15530 in the network. Up to two OSC modules can be installed in the carrier motherboard, one module for the west direction and one for the east direction.

16.2 Initial Troubleshooting Checklist

Follow this initial checklist before proceeding with the troubleshooting procedures:

- Check that the LEDs on the cards show the proper state.
- Verify patch configuration.
- Ensure that all optical connectors are clean. Refer to the *Cisco ONS 15530 Cleaning Procedures for Fiber Optic Connections* document.

16.3 Troubleshooting OSCP Problems

This section contains troubleshooting procedures for OSCP problems.

16.3.1 OSC Wave Interface Down

Symptom The OSC wave interface is down.

Table 16-1 describes the potential causes of the symptom and the solutions.

Table 16-1 OSC Wave Interface Is Down

Possible Problem	Solution
Interface is administratively down.	Issue a show interfaces wave command to verify the OSC wave interface status. If it is administratively down, issue a no shutdown command.
Receive power level is low.	Check the receive power level from the OADM module. Ensure that it is between -19 dBm and -1.5 dBm.
The optical connectors are dirty.	Refer to the <i>Cisco ONS 15530 Cleaning Procedures for Fiber Optic Connections</i> document.
The patch cables are faulty.	Check the patch cables between the OSC module and the OADM module for pinches or breaks. Correct any problems with the fiber.

16.3.2 EthernetDcc Interface Down

Symptom The ethernetdcc interface is down.

Table 16-2 describes the potential causes of the symptom and the solutions.

Table 16-2 EthernetDcc Interface Is Down

Possible Problem	Solution
Interface is administratively down.	Issue a show interfaces wave command to verify the ethernetdcc interface status. If it is administratively down, issue a no shutdown command.
Receive power level is low.	Check the receive power level from the OADM module. Ensure that it is between -19 dBm and -1.5 dBm.
The optical connectors are dirty.	Refer to the <i>Cisco ONS 15530 Cleaning Procedures for Fiber Optic Connections</i> document.
The patch cables are faulty.	Check the patch cables between the OSC module and the OADM module for pinches or breaks. Correct any problems with the fiber.

16.3.3 EthernetDcc Interface Is Up But Line Protocol Is Down

Symptom The EthernetDcc interface is up but line protocol is down.

Table 16-3 describes the potential cause of the symptom and the solutions.

Table 16-3 *EthernetDcc Interface Is Up But Line Protocol Is Down*

Possible Problem	Solution
The remote ethernetdcc interface is shut down.	<ol style="list-style-type: none">1. Issue the show oscp interface command to check the OSCP status.2. If the ethernetdcc interface is in the “attempt” state, issue the show interfaces command on the remote system to determine the administrative state of the ethernetdcc interface. Issue the no shutdown command to bring it up, if necessary.

■ 16.3.3 EthernetDcc Interface Is Up But Line Protocol Is Down



Troubleshooting Threshold Alarms

This chapter describes how to troubleshoot threshold alarm problems. This chapter includes the following sections:

- 17.1 Initial Troubleshooting Checklist, page 17-1
- 17.2 Troubleshooting Threshold Alarms, page 17-1

17.1 Initial Troubleshooting Checklist

Follow this initial checklist before proceeding with the troubleshooting procedures:

- Issue **show interfaces** commands to ensure that all interfaces are administratively up and that there are no reported errors.
- Issue the **show facility-alarm status** command to display the alarms on the interfaces.
- Ensure that all optical connectors are clean. Refer to the *Cisco ONS 15530 Cleaning Procedures for Fiber Optic Connections* document.

17.2 Troubleshooting Threshold Alarms

This section contains troubleshooting procedures for threshold alarm problems. Threshold alarms indicate that a configured range is exceeded.

17.2.1 8b10b CVRD Alarm Indicates Signal Fail or Signal Degrade

Symptom An 8b10b CVRD alarm indicates signal fail or signal degrade.

Table 17-1 describes the potential causes of the symptom and the solutions.

Table 17-1 8b10b CVRD Alarm Indicates Signal Fail or Signal Degrade

Possible Problem	Solution
Excessive attenuation or overloading on a 2.5-Gbps ITU trunk card interface.	<ol style="list-style-type: none"> 1. Measure the receive power level. Ensure that it is within -28 dBm and -8 dBm. Adjust the attenuation if necessary. 2. Check the network cable for sharp bends and ensure the connectors are clean and connected properly. Refer to the <i>Cisco ONS 15530 Cleaning Procedures for Fiber Optic Connections</i> document.
Excessive attenuation or overloading on a 10-Gbps ITU trunk or 10-Gbps ITU tunable trunk interface.	<ol style="list-style-type: none"> 1. Measure the receive power level. Ensure that it is within -22 dBm and -8 dBm. Adjust the attenuation if necessary. 2. Check the network cable for sharp bends and ensure the connectors are clean and connected properly. Refer to the <i>Cisco ONS 15530 Cleaning Procedures for Fiber Optic Connections</i> document.
Excessive attenuation or overloading on an 8-port FC/GE aggregation card interface.	<ol style="list-style-type: none"> 1. Measure the receive power level. Ensure that it is within -18 dBm and -13.5 dBm for a multimode FC/GE interface and within -20.5 dBm and -3 dBm for a single mode FC/GE interface. Adjust the attenuation if necessary. 2. Check the network cable for sharp bends and ensure the connectors are clean and connected properly. Refer to the <i>Cisco ONS 15530 Cleaning Procedures for Fiber Optic Connections</i> document.
Excessive attenuation or overloading on a 10-port ESCON aggregation card interface.	<ol style="list-style-type: none"> 1. Measure the receive power level. Ensure that it is within -33 dBm and -14 dBm. Adjust the attenuation if necessary. 2. Check the network cable for sharp bends and ensure the connectors are clean and connected properly. Refer to the <i>Cisco ONS 15530 Cleaning Procedures for Fiber Optic Connections</i> document.
Excessive attenuation or overloading on an OSC module interface.	<ol style="list-style-type: none"> 1. Measure the receive power level. Ensure that it is within -19 dBm and -1.5 dBm. Adjust the attenuation if necessary. 2. Check the network cable for sharp bends and ensure the connectors are clean and connected properly. Refer to the <i>Cisco ONS 15530 Cleaning Procedures for Fiber Optic Connections</i> document.

17.2.2 CDL HEC Alarm Indicates Signal Fail or Signal Degrade

Symptom A CDL HEC alarm indicates signal fail or signal degrade.

Table 17-2 describes the potential causes of the symptom and the solutions.

Table 17-2 CDL HEC Alarm Indicates Signal Fail or Signal Degrade

Possible Problem	Solution
Excessive attenuation or overloading on an OSC module interface.	<ol style="list-style-type: none"> 1. Measure the receive power level. Ensure that it is within -19 dBm and -1.5 dBm. Adjust the attenuation if necessary. 2. Check the network cable for sharp bends and ensure the connectors are clean and connected properly. Refer to the <i>Cisco ONS 15530 Cleaning Procedures for Fiber Optic Connections</i> document.
Excessive attenuation or overloading on a 10-Gbps ITU trunk card or 10-Gbps ITU tunable trunk card interface.	<ol style="list-style-type: none"> 1. Measure the receive power level. Ensure that it is within -22 dBm and -8 dBm. Adjust the attenuation if necessary. 2. Check the network cable for sharp bends and ensure the connectors are clean and connected properly. Refer to the <i>Cisco ONS 15530 Cleaning Procedures for Fiber Optic Connections</i> document.

17.2.3 64b66b CVRD Alarm Indicates Signal Fail or Signal Degrade

Symptom A 64b66b CVRD alarm indicates signal fail or signal degrade.

Table 17-3 describes the potential causes of the symptom and the solutions.

Table 17-3 64b66b CVRD Alarm Indicates Signal Fail or Signal Degrade

Possible Problem	Solution
Excessive attenuation or overloading on a 10-Gbps ITU trunk card or 10-Gbps ITU tunable trunk card interface.	<ol style="list-style-type: none"> 1. Measure the receive power level. Ensure that it is within -22 dBm and -8 dBm. Adjust the attenuation if necessary. 2. Check the network cable for sharp bends and ensure the connectors are clean and connected properly. Refer to the <i>Cisco ONS 15530 Cleaning Procedures for Fiber Optic Connections</i> document.

17.2.4 B1 CVRD Alarm Indicates Signal Fail or Signal Degrade

Symptom A B1 CVRD alarm indicates signal fail or signal degrade.

Table 17-4 describes the potential causes of the symptom and the solutions.

Table 17-4 B1 CVRD Alarm Indicates Signal Fail or Signal Degrade

Possible Problem	Solution
Excessive attenuation or overloading on a SONET/SDH interface.	<ol style="list-style-type: none"> 1. Measure the receive power level. Ensure that it is within -25 dBm and -8 dBm for a multimode interface and within -19 dBm and -1.5 dBm for a single mode interface. Adjust the attenuation if necessary. 2. Check the network cable for sharp bends and ensure the connectors are clean and connected properly. Refer to the <i>Cisco ONS 15530 Cleaning Procedures for Fiber Optic Connections</i> document.

17.2.5 Threshold Exceeded Messages Continuously Hitting the Console

Symptom Threshold exceeded messages continuously hitting the console.

Table 17-5 describes the potential cause of the symptom and the solution.

Table 17-5 *Threshold Exceeded Messages Continuously Hitting the Console*

Possible Problem	Solution
Receive signal is fluctuating on the edge of the configured threshold.	<ol style="list-style-type: none"> 1. Measure the interface receive power level. Ensure that it is within specifications. Adjust the attenuation if necessary. 2. Check the network cable for sharp bends and ensure the connectors are clean and connected properly. Refer to the <i>Cisco ONS 15530 Cleaning Procedures for Fiber Optic Connections</i> document.

17.2.6 SNMP Traps Are Not Generated

Symptom SNMP traps are not generated.

Table 17-6 describes the potential cause of the symptom and the solution.

Table 17-6 *SNMP Traps Are Not Generated*

Possible Problem	Solution
SNMP configuration is incorrect.	Issue a show running-config command to verify the SNMP configuration and correct if necessary.



Troubleshooting Performance History Counter Problems

This chapter describes how to troubleshoot performance history counter problems. This chapter contains the following sections:

- 18.1 Overview, page 18-1
- 18.2 Initial Troubleshooting Checklist, page 18-1
- 18.3 Interpreting Performance History Messages, page 18-2
- 18.4 Troubleshooting Performance History Counters, page 18-2

18.1 Overview

Cisco ONS 15530 supports 15 minute based performance history counters. You can use the performance history counters to track the performance of the Cisco ONS 15530 interfaces.

There are three types of performance history counters: current, 15-minute history, and 24-hour. Cisco ONS 15530 uses these counters to store the performance data for the following time periods:

- The current 15 minutes (using the current counter).
- The last 24 hours (using ninety six 15-minute history counters).
- The previous 1 day (using the 24-hour counter).

For more information on performance history counters, refer to the *Cisco ONS 15530 Configuration Guide*.

18.2 Initial Troubleshooting Checklist

Follow this initial checklist before proceeding with the troubleshooting procedures:

- Issue the **show version** command to ensure that the IOS version is 12.2(29)SV or later.
- Issue **show interfaces** commands to ensure that the interface for which the performance history counters are being monitored is administratively up.
- Ensure that the encapsulation configured on the interface supports performance history counters.
- To preserve the performance history counters across a CPU switch module switchover, ensure that the `auto-sync counter interfaces` configuration is present in the running configuration.

18.3 Interpreting Performance History Messages

This section explains the informational messages that may be displayed on the command line interface (CLI) while you are working with the performance history counters.

Message	Description
Sorry! Current 15 minute interval [dec] on [interface] just started. Please try again.	This message indicates that the elapsed time and the valid time are equal to zero. This message is displayed if you issue the show performance command immediately after the current counter completes its 15 minute interval.
Sorry! No counters for this interface/encapsulation combination.	This message indicates that the encapsulation configured on the interface does not support performance history counters, or the monitoring of the transparent interfaces is disabled.
Sorry! No valid current 15 minute data for interval [dec] on [interface].	This message indicates that the specified interface was administratively down during the 15 minute interval of the current counter.
Sorry! No valid performance data for interval [dec] on [interface].	This message indicates that the specified interface was administratively down during the entire interval of the performance history counter.
Sorry! No valid 24 hour performance data for [interface].	This message indicates that the interface was administratively down during the full 24 hour interval of the 24-hour counter.
Sorry! 15 minute performance history register [dec] not available for [interface].	This message is displayed if the 15-minute history counter is yet to be created.
Sorry! 24 hour performance register not available for [interface].	This message is displayed if the 24-hour counter is yet to be created.
Sorry! Current 15 minute register not available for [interface].	This message indicates that the specified interface does not support performance history counters.

18.4 Troubleshooting Performance History Counters

This section contains troubleshooting procedures for performance history counter problems.

18.4.1 Some Counters Are Not Displayed

Symptom Some interface counters are not displayed in the output of the **show performance** command.

Table 18-1 describes the potential causes of the symptom and the solutions.

Table 18-1 Some Counters Are Not Displayed

Possible Problem	Solution
Monitoring of the transparent interface of the transponder is disabled.	Issue the monitor enable command to enable monitoring of the transparent interface.
The missing interface counters are not supported by the performance history feature.	Refer to the <i>Cisco ONS 15530 Configuration Guide</i> for the list of interface counters that are supported by the performance history feature.

18.4.2 Performance History Counters Are Not Preserved Across CPU Switch Module Switchovers

Symptom The performance history counters are not preserved across a CPU switch module switchover. Table 18-2 describes the potential causes of the symptom and the solutions.

Table 18-2 Performance History Counters Are Not Preserved Across CPU Switch Module Switchovers

Possible Problem	Solution
Automatic synchronization of performance history counters is not enabled.	Issue the auto-sync counter interfaces command to enable the automatic syncing of the performance history counters to the standby CPU switch module.

■ 18.4.2 Performance History Counters Are Not Preserved Across CPU Switch Module Switchovers



Technical Support

When you have a problem that you cannot resolve, contact customer service. To help resolve these problems, gather relevant information about your network prior to calling. This appendix includes the following sections:

- A.1 Gathering Information About Your Internetwork, page A-1
- A.2 Providing Data to Customer Service, page A-2

A.1 Gathering Information About Your Internetwork

Before gathering any specific data, compile a list of all symptoms users have reported on the internetwork (such as connections dropping or slow host response).

The next step is to gather specific information. Typical information needed to troubleshoot internetworking problems fall into two general categories: information required for any situation and information specific to the topology, technology, protocol, or problem.

Information that is always required by technical support engineers includes the following:

- Configuration listing of all systems involved
- Complete specifications of all systems involved
- Version numbers of software (obtained by using the **show version** command) and Flash code (obtained by using the **show controllers** command) on all relevant systems
- Network topology map
- List of hosts and servers (host and server type, number on network, description of host operating systems that are implemented)
- List of network layer protocols, versions, and vendors

To assist you in gathering this required data, the **show tech-support** EXEC command has been added in Cisco IOS Release 11.1(4) and later. This command provides general information about the system that you can provide to your technical support representative when you are reporting a problem.

The **show tech-support** command display includes outputs from the **show version**, **show hardware**, **show diag power-on**, **show running-config**, **show controllers**, **show stacks**, **show interfaces**, **show buffers**, **show process memory**, and **show process** EXEC commands.

Specific information that might be needed by technical support varies, depending on the situation, and include the following:

- Output from the following general **show** commands:

show interfaces

show controllers [atm | serial | e1 | ethernet]

show processes [cpu | mem]

show buffers

show memory summary

- Output from the following protocol-specific **show** commands:

show protocol route

show protocol traffic

show protocol interface

show protocol arp

- Output from relevant **debug** privileged EXEC commands
- Output from protocol-specific **ping** and **trace** command diagnostic tests, as applicable
- Network analyzer traces, as applicable
- Core dumps obtained by using the **exception dump** switch configuration command, or by using the **write core** switch configuration command if the system is operational, as appropriate

A.1.1 Getting the Data from Your System

When obtaining information from your system, tailor your method to the system that you are using to retrieve the information. Following are some hints for different platforms:

- PC and Macintosh—Connect a PC or Macintosh to the console port of the system and log all output to a disk file (using a terminal emulation program). The exact procedure varies depending on the communication package used with the system.
- Terminal connected to console port or remote terminal—The only way to get information with a terminal connected to the console port or with a remote terminal is to attach a printer to the Aux port on the terminal (if one exists) and to force all screen output to go to the printer. Using a terminal is undesirable because there is no way to capture the data to a file.
- UNIX workstation—At the UNIX prompt, enter the **script filename** command, then use Telnet to connect to the system. The UNIX **script** command captures all screen output to the specified filename. To stop capturing output and close the file, enter the end-of-file character (typically **^D**) for your UNIX system.



Note

To get your system to automatically log specific error messages or operational information to a UNIX syslog server, use the **logging internet-address** switch configuration command. For more information about using the **logging** command and setting up a syslog server, refer to the Cisco IOS configuration guides and command reference publications.

A.2 Providing Data to Customer Service

If you need technical assistance with a Cisco product that is under warranty or covered by a maintenance contract, contact TAC (Cisco's Technical Assistance Center) to open a case. Contact TAC with a phone call or an e-mail message:

- North America: 800-553-2447, e-mail: tac@cisco.com
- Europe: 32 2 778 4242, e-mail: euro-tac@cisco.com
- Asia-Pacific: 61 2 9935 4107, e-mail: asiapac-tac@cisco.com

When submitting information to your technical support representative, electronic data is preferred. Electronic data significantly eases the transfer of information between technical support personnel and development staff. Common electronic formats include data sent via e-mail and files sent using FTP (File Transfer Protocol).

If you are submitting data to your technical support representative, use the following list to determine the preferred method for submission:

1. The preferred method of information submission is through FTP service over the Internet. If your environment supports FTP, you can place your file in the incoming directory on the host cco.cisco.com.
2. The next best method is to send data by electronic mail. Before using this method, be sure to contact your technical support representative, especially when transferring binary core dumps or other large files.

If you use e-mail, do not use encoding methods such as binhex or zip. Only MIME-compliant mail should be used.

3. Use a PC-based communications protocol, such as Kermit, to upload files to Cisco.com. Again, be sure to contact your technical support representative before attempting any transfer.
4. Transfer by disk or tape.
5. The least favorable method is hard-copy transfer by fax or physical mail.



Numerics

10-Gbps ITU trunk cards

interface problems **9-3 to 9-5, 10-3 to 10-5**

interfaces (figure) **9-1**

loopbacks **9-5 to 9-7, 10-6 to 10-7**

overview **9-1**

troubleshooting checklist **9-3, 10-3**

10-Gbps ITU tunable trunk cards

interfaces (figure) **10-1**

overview **10-1**

10-Gbps uplink cards

interface problems **11-2 to 11-3**

interfaces (figures) **11-1**

loopbacks **11-4 to 11-5**

troubleshooting checklist **11-2**

2.5-Gbps ITU trunk cards

interface problems **8-3 to 8-5**

interfaces (figures) **8-1**

loopbacks **8-5 to 8-7**

troubleshooting checklist **8-2, 12-2**

waveethernetphy interface problems **8-3**

4-port 1-Gbps/2-Gbps FC aggregation cards

asymmetric throughput **5-9**

client equipment problems **5-5**

FC problems **5-3, 5-6**

FICON problems **5-3, 5-6**

flow control is inactive **5-10**

interface problems **5-3 to 5-7, ?? to 5-10**

interfaces (figure) **5-2**

loopbacks **5-16 to 5-18**

low throughput **5-8**

oversubscription problems **5-10**

superportgroup problems **5-10**

troubleshooting checklist **5-2**

twogigabit interface problems **5-7**

twogigabitphy interface not created **5-7**

twogigabitphy interface problems **5-3, 5-5**

twogigabitphy interface reports Loss of Sync **5-8**

8-port FC/GE aggregation cards

client equipment problems **6-5**

FC problems **6-3, 6-7**

FICON problems **6-3, 6-7**

GE problems **6-3**

gigabit interface problems **6-8**

gigabitphy interface not created **6-8**

gigabitphy interface problems **6-4, 6-6**

interface problems **6-3 to 6-8**

interfaces (figure) **6-2**

loopbacks **6-11 to 6-12**

troubleshooting checklist **6-2**

8-port multi-service muxponders

interfaces (figure) **7-2**

loopbacks **7-10 to 7-14**

overview **7-1**

terminal loopbacks **7-11, 7-12**

troubleshooting

 multirate interface problems **7-2 to 7-6**

 sdcc interface problems **7-8**

 wavesonetphy interface problems **7-7 to 7-8**

troubleshooting checklist **7-2**

TSI mapping problems **7-9**

A

accessibility tests **1-8**

- APS
- bidirectional problems 15-2
 - group not associated 15-2
 - interfaces down 15-6
 - lockout fails 15-4
 - message channel problems 15-3
 - switchover fails 15-4, 15-5, 15-6
 - transmit k1k2 sf-lp 15-6
 - troubleshooting checklist 15-1
 - troubleshooting problems 15-2 to 15-7
- Automatic Protection Switching. See APS
-
- B**
- bit error rate tester 1-5
 - booting
 - redundant CPU switch modules 2-15
 - Bug Toolkit
 - searching DDTs database 1-17
-
- C**
- Cisco.com
 - uploading files to A-3
 - Cisco IOS images. See system images
 - Cisco TAC. See TAC
 - Cisco Transport Manager. See CTM 1-4
 - CiscoView 1-4
 - client equipment problems
 - detects CVRD errors 5-5, 6-5
 - configuring online diagnostic tests 1-9 to 1-16
 - CPU switch modules
 - active CPU switch module boot failure 2-22
 - console cannot be accessed 2-23
 - displaying configuration 2-2
 - overview 2-1
 - recovering passwords 2-4
 - software compatibility 2-13
 - standby CPU switch module boot failure 2-23
 - troubleshooting checklist 2-2
 - troubleshooting memory 2-9
 - troubleshooting redundant 2-15
 - unable to access enable mode 2-23
 - verifying 2-2
 - verifying hardware and software compatibility 2-13
 - verifying hardware and software versions 2-9
 - verifying NME interface configurations 2-5
 - CTM 1-4
 - customer service and support. See TAC
-
- D**
- DDTs
 - using Bug Toolkit 1-17
 - debug commands
 - cautions 1-7
 - ping command 1-7
 - traceroute command 1-7
 - debug diag online command 1-9
 - Device Fault Manager. See DFM
 - DFM 1-5
 - diagnostic commands
 - types 1-6 to 1-8
 - diag online command 1-9, 1-11
 - diag online subslot command 1-9
 - documentation
 - related xxi
-
- E**
- echo messages. See ICMP echo messages
 - error message logging. See message logging
 - ESCON aggregation cards
 - client side interface problems 4-3, 4-4
 - esconphy interface not created 4-6
 - esconphy interface problems 4-4

- interface problems **4-3 to 4-6**
- interfaces **4-1**
- interfaces (figure) **4-2**
- overview **4-1**
- signal path (figure) **4-1, 14-1**
- traffic flow problems **4-5**
- troubleshooting checklist **4-2**
- using loopbacks **4-7**

esconphy interfaces

- all client side lasers down **4-4**
- not created **4-6**
- removing SFP optics **4-3**
- shutting down **4-3**
- unexpectedly shuts down **4-4**

ethernetdcc interfaces down

- 10-Gbps ITU trunk cards **9-5, 10-5**
- 10-Gbps uplink cards **11-3**
- 2.5-Gbps ITU trunk cards **8-5**
- OSC modules **16-2**

F

- facility loopbacks **5-16, 6-11, 7-10, 7-11, 8-5, 8-6**
- fiber microscope **1-5**
- fixed attenuators **1-5**
- FTP
 - sending data to TAC **A-3**

G

general troubleshooting

- internetwork maps **1-4**
- problem-solving models (figure) **1-3**
- problem-solving steps **1-3**
- tools **1-5 to 1-6**

gigabitphy interfaces

- administratively down **6-4**
- CRC errors **6-7**

- local and remote down **6-8**

- Loss of Light **5-3, 6-3**

- Loss of Sync **6-3**

- not created **6-8**

- transmit frame count not incrementing **6-6**

H

hardware

- confirming integrity of **1-18**
- verifying versions **2-9 to 2-12**

I

- ICMP echo messages **1-7**

- Internet Control Message Protocol echo messages. See ICMP echo messages

- internetwork maps. See network maps

K

Kermit protocol

- providing data to TAC **A-3**

L

LEDs

- VOA module problems **14-6**

- logging command **A-2**

M

Macintosh

- logging system output **A-2**

- maintaining network information **1-4**

memory

- troubleshooting CPU switch module **2-9**

message logging

- choosing destinations **A-2**

syslog servers **A-2**

N

network and system management

tools supported **1-4**

network management Ethernet ports. See NME

network maps

preparing for failures **1-4**

network monitoring

CiscoView **1-4**

network monitors **1-6**

network performance

debug commands (caution) **1-7**

NME

displaying interface configurations **2-5**

troubleshooting connections **2-5**

no debug all command **1-7**

no debug command **1-7**

O

OADM modules

architecture (figure) **12-2**

description **12-1**

OIR tests **1-9**

online diagnostics

accessibility tests **1-8**

configuring **1-8, 1-9**

displaying **1-10**

displaying configuration **1-10, 1-12**

optical cleaning kit **1-5**

optical power meter **1-5**

optical supervisory channel

overview **16-1**

optical time domain reflector/reflectometer **1-5**

OSC modules

ethernetdcc interface is down **16-2**

line protocol is down **16-2**

overview **16-1**

troubleshooting checklist **16-1**

wave interface is down **16-2**

P

passwords

recovering **2-4 to 2-5**

patch cables **1-5**

PB-OE modules

interfaces (figure) **14-2, 14-3**

STA LED problems **14-6**

troubleshooting checklist **14-3**

voafilterin subinterface problems **14-4**

warnings not reported **14-6**

PCs

logging system output **A-2**

performance. See network performance

performance history counters

description **18-1**

interpreting messages **18-2**

not preserved across CPU switchovers **18-3**

some counters are not displayed **18-2**

troubleshooting checklist **18-1**

problem solving

process **1-3**

Protection switch module. See PSM

PSM

interface problems **13-1**

troubleshooting checklist **13-1**

R

recovering passwords **2-4**

redundancy

troubleshooting CPU switch modules **2-15 to 2-22**

release notes

checking for workarounds **1-17**
 remote terminals
 logging system output **A-2**

S

script command (UNIX) **A-2**
 security password recovery **2-4 to 2-5**
 SFP optics
 8-port FC/GE aggregation cards **6-1**
 show buffers command **1-6, 2-9, 2-23, A-1**
 show controllers command **1-6, 2-6, 2-7, 5-11, 6-9, A-2**
 show flash command **1-6**
 show hardware detail command **2-16**
 show interfaces command **1-6, 2-6, 3-4, 3-5, 3-6, 3-8, 4-2, 4-5, 5-2, 5-4, 5-5, 5-6, 5-7, 6-2, 6-5, 6-6, 6-7, 6-8, 7-6, 8-2, 8-3, 8-4, 8-5, 9-3, 9-4, 9-5, 10-3, 10-4, 10-5, 11-2, 11-3, 12-2, 12-3, 14-3, 14-4, 14-5, 14-6, 15-1, 15-3, 15-5, 15-7, 16-2, 17-1**
 show memory command **1-6, 2-9, A-2**
 show processes command **1-6, A-2**
 show redundancy capability command **2-16**
 show running-config command **1-6, 2-2, 12-3, 17-4, A-1**
 show stacks command **1-7, A-1**
 show startup-config command **1-6, 2-5**
 show tech-support command **A-1**
 show version command **1-7, 2-4, 2-9, 2-16, A-1**
 software
 checking for bug workarounds **1-16**
 compatibility **2-13**
 downloading from Cisco.com **2-22**
 verifying versions **2-9**
 spectrum analyzer **1-6**
 SPF optics
 ESCON aggregations cards **4-1**
 support, technical. See TAC
 switch fabric **2-1**
 syslog servers **A-2**
 system images
 checking release notes **1-16**

T

TAC
 contacting **A-2**
 gathering data for **A-1 to A-2**
 providing data to **A-3**
 show tech-support command **A-1**
 Technical Assistance Center. See TAC
 technical support. See TAC
 tengigethernetphy interfaces
 Loss of Lock **11-3**
 Loss of Sync **11-3**
 terminal loopbacks **5-16, 5-17, 6-11, 6-12, 7-10, 8-5, 8-6, 9-5, 9-6, 10-6, 10-7, 11-4, 11-5**
 terminals. See remote terminals
 threshold alarms
 64b66b CVRD alarm **17-3**
 8b10b CVRD alarm **17-1**
 B1 CVRD alarm **17-3**
 CDL HEC alarm **17-2**
 continuous threshold exceeded messages **17-4**
 troubleshooting checklist **17-1**
 time domain reflectometer **1-5**
 traceroute command **1-8**
 transparent interfaces
 Loss of Frame **3-6**
 Loss of Light **3-4**
 Loss of Lock **3-5**
 Loss of Sync **3-5**
 transponder line cards
 architecture **3-2**
 interfaces **3-2**
 Loss of Frame **3-6**
 Loss of Light **3-3, 3-4**
 Loss of Lock **3-5**
 Loss of Sync **3-5**
 low alarm **3-6**
 not listed **3-3**
 overview **3-1**

- rejects clock rate **3-6**
- rejects protocol encapsulation **3-6**
- troubleshooting checklist **3-2**
- troubleshooting checklists
 - 10-Gbps ITU trunk cards **9-3, 10-3**
 - 10-Gbps uplink cards **11-2**
 - 2.5-Gbps ITU trunk cards **8-2, 12-2**
 - 4-port 1-Gbps/2-Gbps FC aggregation cards **5-2**
 - 8-port FC/GE aggregation cards **6-2**
 - 8-port multi-service muxponders **7-2**
 - APS **15-1**
 - CPU switch modules **2-2**
 - ESCON aggregation cards **4-2**
 - OSC **16-1**
 - PSM **13-1**
 - threshold alarms **17-1**
 - transponder line cards **3-2**
 - VOA modules **14-3**
- troubleshooting tools
 - bit error rate tester **1-5**
 - fiber microscope **1-5**
 - fixed attenuators **1-5**
 - network monitors **1-6**
 - optical cleaning kit **1-5**
 - optical power meter **1-5**
 - optical time domain reflector/reflectometer **1-5**
 - patch cables **1-5**
 - spectrum analyzer **1-6**
 - time domain reflectometer **1-5**
- twogigabitphy interfaces
 - administratively down **5-3**
 - asymmetric throughput **5-9**
 - CRC errors **5-6**
 - flow control is inactive **5-10**
 - local and remote down **5-7**
 - Loss of Sync **5-8**
 - low throughput **5-8**
 - not created **5-7**
 - transmit frame count not incrementing **5-5**

U

UNIX

- logging system output **A-2**
- script command **A-2**

V

voafilterin subinterfaces

- high optical threshold error **14-5**
- low optical threshold error **14-4**

voain interfaces

- high optical threshold error **14-5**
- low optical threshold error **14-4**

VOA modules

- interface problems **14-3**
- interfaces (figure) **14-1, 14-2**
- STA LED problems **14-6**
- troubleshooting checklist **14-3**
- types **14-1**
- warnings not reported **14-6**

W

waveethernetphy interfaces

- 10-Gbps ITU trunk cards
 - Loss of Lock **9-3, 10-3**
 - Loss of Sync **9-4, 10-4**
- 2.5-Gbps ITU trunk cards
 - Loss of Lock **8-3**
 - Loss of Sync **8-3**

wave interfaces

- Loss of Frame **3-6**
- Loss of Light **3-3**
- Loss of Lock **3-5**
- Loss of Sync **3-5**

wavepatch interfaces

- Loss of Light **3-4**
- low alarm **3-6**

wavesonetphy interfaces**Loss of Frame 7-8****Loss of Lock 7-7****Loss of Signal 7-7****WB-VOA modules****interfaces (figure) 14-1, 14-2****STA LED problems 14-6****troubleshooting checklist 14-3****voain interface problems 14-4, 14-5****warnings not reported 14-6****workarounds****checking release notes 1-16**